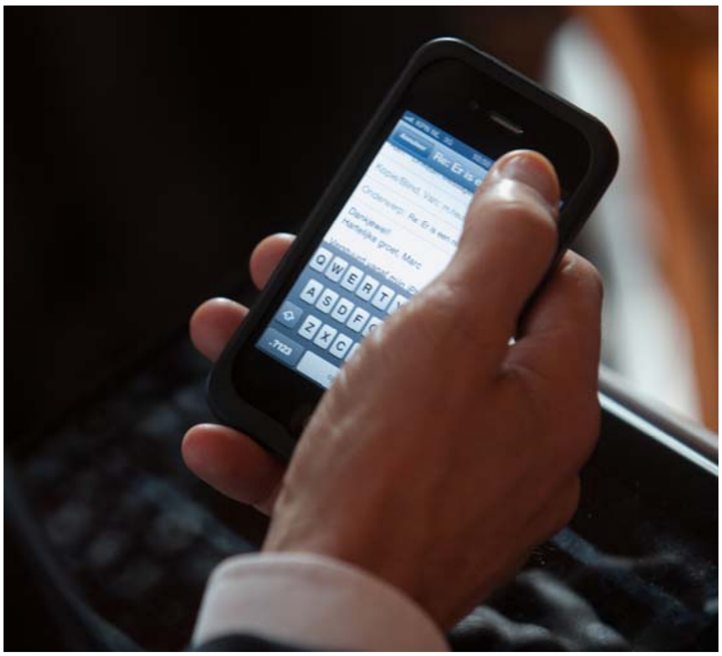
De bewaarplicht telecomgegevens en de opsporing

Het belang van historische telecommunicatie gegevens voor de opsporing



Mr. W.N. Ferdinandusse, officier van justitie bij het Landelijk Parket
Mr. D. Laheij, landelijk officier van justitie interceptie bij het Landelijk Parket
Mr. J.C. Hendriks, hoofdinspecteur bij de Nationale Politie
23 maart 2015

POLITIE
OPENBAAR MINISTERIE

INHOUDSOPGAVE

Woord vooraf

In dit rapport geven Openbaar Ministerie en politie informatie over het gebruik van historische telecommunicatie gegevens (gebruikers- en verkeersgegevens en locatie gegevens) van (mobiele) telefonie en internet bij de opsporing en vervolging van daders van ernstige strafbare feiten. Dit rapport is vooral geschreven om belangstellenden meer inzicht te geven in het belang van dergelijke gegevens en de bewaarplicht daarvan, bij de aanpak van ernstige criminaliteit.

In de huidige samenleving, waarin zoveel communicatie plaatsvindt via telefoon en internet, zijn er eigenlijk geen alternatieven denkbaar voor het gebruik van (historische) telecommunicatiegegevens in de opsporing. In een toenemend aantal gevallen vormen gebruikers- en verkeersgegevens het enige aanknopingspunt voor de opsporing. Denk bijvoorbeeld aan veel vormen van computercriminaliteit, maar ook het bezit en de verspreiding van kinderporno en uitingsdelicten als discriminatie, smaad en bedreiging. Maar ook bij veel straatroven en inbraken zijn verkeersgegevens (die aangeven wie, waar, wanneer was en met wie contact had) vaak het voornaamste aanknopingspunt.

Zonder bewaarplicht voor telecommunicatiegegevens verwachten wij dat de effectiviteit en efficiëntie bij het opsporen en vervolgen van ernstige misdrijven aanzienlijk zal dalen. Daarmee zou de overheid in een belangrijke verplichting jegens haar burgers tekortschieten. Het recht op eerbiediging van het privéleven geldt immers ook voor slachtoffers van misdrijven, die er recht op hebben dat de overheid hen beschermt tegen de risico's en gevolgen van criminaliteit door adequate mogelijkheden te creëren om daders daarvan op te sporen en te bestraffen.

Telecommunicatiegegevens worden alleen opgevraagd bij de aanbieder nadat in de concrete zaak bij iedere bevraging steeds weer een afweging is gemaakt tussen de inbreuk op de privacy en het belang van de gegevens voor de opsporing en de officier van justitie van oordeel is dat de bevraging proportioneel is en er geen andere mogelijkheden zijn om aan de desbetreffende gegevens te komen.
Politie en OM erkennen het belang en de noodzaak van een goede balans tussen de bescherming van de persoonlijke levenssfeer (het recht op privacy) enerzijds en de bescherming van de maatschappij tegen ernstige criminaliteit anderzijds. Privacy van der burger is een groot goed, de effectieve opsporing en vervolging van ernstige misdrijven is dat ook. De overheid heeft de publieke taak om misdrijven op te sporen en op te lossen. Zowel in de fysieke als in de virtuele wereld moeten mensen zich veilig kunnen begeven en daar waar mogelijk worden beschermd tegen criminaliteit. Telecommunicatiegegevens spelen daarbij een cruciale rol. Daarbij kunnen conflicterende belangen een rol spelen, bescherming van het ene grondrecht kan met zich meebrengen dat het noodzakelijk is om inbreuk te maken op een ander grondrecht, waarbij steeds weer in het concrete geval een afweging moet worden gemaakt. Inbreuk op het grondrecht van privacy kan soms aangewezen zijn om grovere inbreuken op andere grondrechten (recht op onaantastbaarheid van het lichaam, huisrecht, onschendbaarheid van het lichaam, verbod op vrijheidsontneming en verbod op discriminatie) op te sporen en de dader daarvan te vervolgen of schending van dat grondrecht tegen te gaan of te laten stoppen.

R. Bik, plaatsvervangend korpschef Nationale Politie.
G.W. van der Burg, procureur-generaal Openbaar Ministerie.

Samenvatting

In dit gezamenlijke rapport beschrijven Openbaar Ministerie en politie het gebruik van historische telecomgegevens en het belang van een bewaarplicht voor zulke gegevens ten behoeve van de opsporing van ernstige strafbare feiten. Dankzij historische telecomgegevens kan vaak worden achterhaald wie waar welk telefoonnummer of IP-adres wanneer in gebruik had. De Wet Bewaarplicht Telecommunicatiegegevens bepaalt dat telefoongegevens 12 maanden moeten worden bewaard en internetgegevens 6 maanden. De rechter heeft op 11 maart 2015 de bewaarplicht buiten werking gesteld. Sindsdien zijn telecomaanbieders niet meer verplicht telecomgegevens te bewaren ten behoeve van de opsporing.

Hoofdstuk 1 beschrijft wat de bewaarplicht inhoudt en om wat voor gegevens het gaat. Telecommunicatiegegevens werden door iedere aanbieder zelf bewaard. Het Agentschap Telecom hield toezicht op de wijze waarop dat bewaren door de aanbieders gebeurde. OM en politie hadden en hebben dus geen grote centrale databakken waar zij naar believen in kunnen zoeken. De gegevens kunnen alleen bij de aanbieders worden gevorderd voor de opsporing en vervolging van ernstige strafbare feiten waarvoor voorlopige hechtenis is toegelaten. De officier van justitie beslist daarover en weegt daarbij de proportionaliteit en subsidiariteit van het gebruik van deze gegevens af.

In de hoofdstukken 2 en 3 wordt aan de hand van meer dan honderddertig gepubliceerde en ongepubliceerde vonnissen uit de afgelopen jaren beschreven hoe historische telecomgegevens worden gebruikt voor de opsporing en vervolging van vele ernstige strafbare feiten. Het gaat daarbij onder meer om moord, doodslag, gewelddadige woningovervallen, verkrachting, mensenhandel, gijzelingen, afpersingen, criminele organisaties die zich bezig houden met drugshandel, diefstallen en fraude, woninginbraken, belaging (*stalking*), bommeldingen met grote gevolgen voor de openbare orde, terroristische misdrijven, kinderporno, online misbruik van kinderen en allerlei vormen van cybercrime. Daarbij kunnen historische telecomgegevens niet alleen belastend bewijs, maar ook belangrijk ontlastend bewijs vormen. Daarom zijn niet alleen de historische telecomgegevens van verdachten belangrijk, maar ook die van bij voorbeeld slachtoffers en van personen die ten onrechte beschuldigd worden.

Hoofdstuk 3 beschrijft waarom het belang van historische telecomgegevens voor de opsporing en vervolging niet in cijfers of statistieken is uit te drukken:

- omdat maar een klein deel van alle rechterlijke uitspraken wordt gepubliceerd;
- omdat gepubliceerde vonnissen meestal niet expliciet ingaan op het gebruik van historische telecomgegevens, ook als dat in het onderzoek wel van groot belang is geweest;
- omdat historische telecomgegevens vaak resultaat opleveren in combinatie met andere opsporingsmiddelen (zoals bijvoorbeeld observeren, doorzoeken van plaatsen, en telefoontaps) waarbij dat resultaat niet achteraf toegeschreven kan worden aan één specifiek opsporingsmiddel;
- omdat politie, Openbaar Ministerie en de rechter van mening kunnen verschillen over de bewijskracht van historische telecomgegevens, en nooit inzichtelijk is of

historische telecomgegevens aan de overtuiging van de rechter hebben bijgedragen (ook als die gegevens niet voor het bewijs worden gebruikt);

- omdat opsporing gericht is op waarheidsvinding en niet alleen op het krijgen van veroordelingen, en het gebruik van historische telecomgegevens dus ook nuttig kan zijn geweest om vast te stellen dat een onderzoek niet moet leiden tot een vervolging;
- omdat historische telecomgegevens niet alleen belangrijk zijn voor het verzamelen van bewijs in Nederlandse strafzaken, maar ook bij het verlenen van rechtshulp aan andere landen en het opsporen van voortvluchtigen. De resultaten daarvan zijn in Nederlandse vonnissen niet terug te vinden;

In hoofdstuk 4 wordt uitgelegd waarom op grond van de ervaringen in verschillende andere Europese landen en uitlatingen van telecomaanbieders zelf valt te verwachten dat zonder bewaarplicht historische telecomgegevens die belangrijk zijn voor de waarheidsvinding aanzienlijk minder vaak beschikbaar zullen zijn voor de opsporing en vervolging.

In hoofdstuk 5 wordt besproken waarom het voor de opsporing vaak nodig is historische telecomgegevens op te vragen van langere tijd geleden en het daarom van belang is telecomgegevens gedurende langere tijd op te slaan. Daarbij wordt toegelicht waarom een bewaartermijn van 6 maanden voor internetgegevens er al regelmatig toe leidt dat meldingen over kinderporno via internet niet onderzocht kunnen worden.

In hoofdstuk 6 worden verschillende andere vragen over de bewaarplicht besproken, bijvoorbeeld waarom het van belang is de telecomgegevens van alle burgers op te slaan en waarom daar geen minder ingrijpende alternatieven voor zijn.

Hoofdstuk 1. De bewaarplicht voor telecomgegevens

De Wet Bewaarplicht Telecommunicatiegegevens bepaalt dat telecommunicatiegegevens 12 maanden worden bewaard waar het telefoniegegevens betreft en 6 maanden waar het Internetgegevens betreft. Deze gegevens zijn alleen in de daarvoor in het Wetboek van Strafvordering omschreven gevallen en onder de daar voorgeschreven voorwaarden beschikbaar voor opsporing en vervolging.

De gegevens kunnen door de politie - op vordering van de officier van justitie - worden opgevraagd bij de aanbieders (providers) en vervolgens worden gebruikt voor de opsporing en vervolging van ernstige misdrijven. Met ernstige misdrijven worden bedoeld de in artikel 67 Wetboek van Strafvordering genoemde misdrijven waarvoor voorlopige hechtenis is toegelaten.

Op 11 maart 2015 heeft de kortgedingrechter in Den Haag de Wet Bewaarplicht Telecommunicatiegegevens zonder terugwerkende kracht buiten werking gesteld.[1] Dat betekent dat aanbieders vanaf die datum niet meer verplicht zijn om de in de wet genoemde telecommunicatiegegevens te bewaren ten behoeve van de opsporing van misdrijven.

Wat zijn nu precies die telecommunicatiegegevens? Telecommunicatiegegevens omvatten de gebruikersgegevens, de verkeersgegevens en de locatiegegevens. Gebruikersgegevens zijn die gegevens die nodig zijn om de abonnee of gebruiker van de communicatiedienst te identificeren zoals naam en adres van de telefoon- of internetabonnee. Verkeersgegevens zijn gegevens die worden verwerkt voor het overbrengen van communicatie zoals gegevens over de datum, het tijdstip en de duur van de communicatie. Locatiegegevens zijn gegevens waarmee de geografische positie van de communicatieapparatuur kan worden bepaald aan de hand van de gebruikte zendmast.
Dankzij verkeers- en gebruikersgegevens kan worden achterhaald wie welk telefoonnummer of IP-adres op welk moment in de tijd in gebruik had. Verkeersgegevens telefonie laten zien welk nummer belde of sms'te met welk nummer en waar. Dus niet wat iemand zegt of sms't. Voor IP-gegevens geldt dat alleen de log-on- en log-off-gegevens worden bewaard. Er wordt dus niet bewaard welke sites worden bezocht, wat er werd geappt, gechat of geskypet, wat werd gegoogled of welke internetaankopen er werden gedaan. Alleen hoe laat en waar werd ingelogd met een (mobiel) device en van welk IP-adres er toen gebruik werd gemaakt. De telecomgegevens geven dus geen inzicht in surfgedrag en ze bevatten evenmin de inhoud van telefoongesprekken of de activiteiten verricht op het internet.

De telecommunicatiegegevens werden door iedere aanbieder zelf bewaard. Het Agentschap Telecom hield toezicht op de wijze waarop dat bewaren gebeurde. Het is dus niet zo dat de gegevens van alle burgers in grote bakken centraal werden bewaard en dat deze gegevens naar believen konden worden geanalyseerd (*data mining*, *profiling*) door politie en justitie. Politie en OM konden en kunnen die gegevens niet zo maar bevragen en analyseren, maar er moet in ieder concreet geval sprake zijn van een verdenking van

[1] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2015:2498

een ernstig misdrijf. Er wordt alleen bevraagd nadat er in een concrete zaak een afweging is gemaakt tussen de privacyschending en het belang van de gegevens voor de opsporing en wanneer de officier van justitie van oordeel is dat de bevraging proportioneel is en er geen andere (minder privacy schendende) manieren zijn om in die zaak de benodigde informatie te verkrijgen.

Aanbieders hebben uiteraard nog wel bepaalde gegevens van hun klanten. De gegevens die nodig zijn voor een goede bedrijfsvoering zoals facturering, klachtafhandeling en gegevens die nodig zijn om de technische staat van de telecom- en internetinfrastructuur te bewaken hebben aanbieders uiteraard nog wel. De officier van justitie kan deze gegevens op grond van het Wetboek van strafvordering nog steeds vorderen.

Afhankelijk van het feit of er tegen het vonnis van de kortgedingrechter appel wordt ingesteld, betekent het vonnis in ieder geval dat er gedurende een bepaalde periode geen gegevens worden opgeslagen in het kader van de bewaarplicht voor de opsporing van ernstige misdrijven. De gegevens die het OM nog wel kan vorderen op grond van het Wetboek van strafvordering zijn gegevens die aanbieders voor hun eigen bedrijfsvoering opslaan. Dit zijn naar hun aard minder gegevens dan in het kader van de Wet bewaarplicht moeten worden opgeslagen en deze worden gedurende een kortere periode bewaard.

Hoofdstuk 2. Historische telecomgegevens in de opsporing

Inleiding

De opsporing van strafbare feiten bestaat voor een belangrijk deel uit het vaststellen *wat* personen *waar* en *wanneer* hebben gedaan, en met *wie*. Voor al die vaststellingen zijn telecomgegevens bruikbaar: zij geven inzicht in contacten, activiteiten en de plaatsen waar personen aanwezig waren. Zij worden dan ook gebruikt voor de opsporing van vele verschillende soorten ernstige misdrijven.

Er bestaan verschillende rapporten die een duidelijk beeld geven van de wijze waarop historische telecomgegevens gebruikt worden in de opsporing, en met welk resultaat. Zo is er een evaluatierapport uit 2012 over de bewaarplicht door het WODC[2], een evaluatie van de Europese Commissie uit 2011[3], en zijn er verschillende documenten van onder meer de Engelse regering,[4] de Duitse politie[5] en de Europese Commissie[6] waarin aan de hand van voorbeelden uit de praktijk wordt toegelicht wat het belang is van het bewaren van telecomgegevens voor de opsporing. In dit rapport wordt de informatie uit de genoemde bestaande rapporten niet herhaald: wie zich een goed beeld wil vormen kan zelf (via de links in de voetnoten) eenvoudig kennis nemen van deze eerdere rapporten.

Ook in de Nederlandse strafrechtspraktijk van de afgelopen jaren zijn vele voorbeelden te vinden van onderzoeken waarin historische telecomgegevens van groot belang zijn geweest voor de opsporing en bewijsvoering. Het gaat daarbij om vele en uiteenlopende ernstige misdrijven, van spraakmakende moorden tot belaging, en van het bedreigen van politici tot gewelddadige woningovervallen.

In het onderstaande overzicht is waar mogelijk verwezen naar openbare bronnen, zodat de lezer daar zelf zo veel mogelijk kennis van kan nemen

Levensdelicten

'Sjaalmoord' Limburg.
Op 11 maart 2015 - dezelfde dag waarop een civiele rechter de bewaarplicht buiten werking stelde - veroordeelde een strafrechter in Limburg[7] een vrouw tot achttien jaar gevangenisstraf voor wat in de pers de 'sjaalmoord' wordt genoemd.[8] De vrouw heeft een

---

[2] Zie https://www.wodc.nl/onderzoeksdatabase/evaluatie-wet-bewaarplicht-telecommunicatiegegevens.aspx.
[3] Zie http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF.
[4] Zie https://www.gov.uk/government/publications/protecting-the-public-in-a-changing-communications-environment.
[5] Zie http://www.bka.de/nn_234056/SharedDocs/Downloads/DE/ThemenABisZ/Mindestspeicherfristen/101008PresseinformationMindestspeicherfristen,templateId=raw,property=publicationFile.pdf/101008PresseinformationMindestspeicherfristen.pdf.
[6] Zie http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf.
[7] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBLIM:2015:2008.
[8] Zie bijv. http://www.1limburg.nl/18-jaar-cel-voor-sjaalmoord-kerkrade.

vrouw van 82 jaar oud in haar eigen huis met een sjaal gewurgd om daarna haar goederen te stelen. Historische telefoongegevens toonden contact aan tussen verdachte en slachtoffer, en tussen twee verdachten onderling rondom het misdrijf. Ter zitting beschuldigde de verdachte vrouw haar medeverdachte om zichzelf vrij te pleiten. Die beschuldiging wordt door de rechtbank verworpen mede op grond van de historische telefoongegevens, waarna de vrouw wordt veroordeeld.

Doodslag bij diefstal Weert.
Op 6 februari 2015 veroordeelt de rechtbank Limburg een man tot vijftien jaar cel voor doodslag en diefstal.[9] De dader heeft een bekende volgens de rechtbank op lafhartige wijze door het achterhoofd geschoten om hem te kunnen beroven. De rechtbank gebruikt historische telefoongegevens van de dader en het slachtoffer voor het bewijs, en stelt daarmee hun aanwezigheid op de plaats delict alsmede het vermoedelijke tijdstip van overlijden van het slachtoffer vast.

Liquidaties Amsterdam: Benaouf A.
Op 1 december 2014 wordt Benaouf A. veroordeeld voor medeplichtigheid aan een liquidatie in Antwerpen die wel wordt gezien als het begin van de huidige reeks onderlinge afrekeningen tussen veelal Amsterdamse criminelen.[10] Blijkens het vonnis waren historische telefoongegevens doorslaggevend, zowel voor het bewijs tegen de dader als voor de weerlegging van een door hem opgevoerd alternatief scenario.
Na de moord wordt in de bosjes bij de plaats delict een prepaidtelefoon gevonden die daar vermoedelijk is weggegooid door iemand uit het gezelschap van het slachtoffer. Op die telefoon zit een briefje met een telefoonnummer van een andere prepaidtelefoon. Beide nummers blijken alleen contact te hebben gehad met elkaar en een derde prepaidtelefoon. Alle drie de telefoons zijn samen gekocht op dezelfde plaats, en alleen gebruikt op de dag van de liquidatie. Uit SMS-berichten aangetroffen in de telefoons blijkt dat zij zijn gebruikt om te communiceren voor de liquidatie.
Vergelijking van de weg die een van de prepaidtelefoons op de dag van de liquidatie heeft afgelegd in België (aan de hand van de aangestraalde telefoonmasten) met de weg die een BMW die dag heeft gereden, die een week later brandend is aangetroffen in Amsterdam, wijst uit dat de telefoon zich in de BMW bevond. Aan de hand van in de BMW aangetroffen DNA, een getuigenverklaring en de historische gegevens van een andere door de verdachte gebruikte telefoon stelt de rechtbank vast dat Benaouf A. de gebruiker was van zowel de BMW als de prepaidtelefoon, en dus betrokken was bij de liquidatie.
Benaouf A. wordt op 10 juni 2013 aangehouden. Hij beroept zich eerst lange tijd op zijn zwijgrecht. Pas zeven maanden na zijn aanhouding legt hij een verklaring af waarin hij uitgebreid een scenario schetst dat hij onschuldig is, en een inmiddels overleden andere persoon aanwijst als de gebruiker van de BMW op de dag van de liquidatie in oktober 2012. Doordat de historische telefoongegevens van zowel enkele familieleden van de verdachte die een rol spelen in zijn alternatieve scenario als de veronderstelde andere gebruiker van de BMW lange tijd na de liquidatie nog opgevraagd kunnen worden, kan de rechtbank vaststellen dat die andere persoon ten tijde van de liquidatie in Amsterdam

---

[9] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBLIM:2015:999.
[10] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2014:8047.

was, en niet in Antwerpen, en dat de verdachte ook over de plaats van zijn familieleden niet de waarheid heeft gesproken. Benaouf A. wordt veroordeeld tot tien jaar gevangenisstraf.

De "Tattoo killers".

Op 18 november 2014 werden vier mannen veroordeeld in hoger beroep voor poging tot moord en voorbereiding daarvan.[11] De mannen worden verdachte van meerdere moorden en worden in de media wel de tattoo killers genoemd. De meesten van hen werden in augustus 2009 aangehouden, kort na een mislukte liquidatiepoging waarbij het slachtoffer door tien kogels werd getroffen maar desondanks overleefde. Na de aanhoudingen werden op verschillende adressen meerdere prepaidtelefoons gevonden. Uit de historische gegevens van die telefoons bleek dat zij alleen contact hadden met elkaar (het Hof spreekt van een gesloten telecomcircuit), en dat zij in de dagen tot aan de liquidatiepoging vele malen gebruikt werden bij de uiteindelijke plaats delict en andere adressen uit de sociale omgeving van het slachtoffer. Het Hof gaat in zijn arrest zeer uitgebreid in op de telecomgegevens en gebruikt die, naast ander bewijs zoals observaties en camerabeelden, om de verdachten als medeplegers te veroordelen tot lange gevangenisstraffen.

De Purmerland moorden.

Ook de veroordeling in 2014 van verschillende daders voor de drievoudige moord in Purmerland steunt voor een belangrijk deel op historische telefoongegevens.[12] Met behulp van telefoongegevens kunnen de verplaatsingen en onderlinge contacten tussen de verschillende verdachten in de periode rondom de moorden worden vastgesteld. De rechtbank verricht die reconstructie in haar vonnis uitgebreid en in groot detail, en verwijst daarbij meer dan zeventig keer naar het telecomdossier. De rechtbank gebruikt de telefoongegevens ook als objectief bewijs om de juistheid van verklaringen te controleren.[13] De rechtbank veroordeelt vier daders tot gevangenisstraffen van tien tot twintig jaar.[14]

TBS voor doodslag op vriendin.

Op 25 juli 2013 wordt een man veroordeeld tot negen jaar gevangenisstraf en TBS voor doodslag op zijn vriendin. Haar lichaam werd aangetroffen in het Rijn-Schiekanaal. Telefoongegevens van zowel verdachte als slachtoffer waren belangrijk voor de opsporing en het bewijs.[15]

Poging doodslag tegen politie bij achtervolging.

Een onbekende bestuurder die levensgevaarlijk heeft gereden en heeft geprobeerd achtervolgende politieagenten te laten verongelukken wordt getraceerd aan de hand van

---

[11] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHAMS:2014:4776.
[12] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBNHO:2014:6284.
[13] Zie o.a. r.o. 4.2.2 en 4.2.9.
[14] Zie http://www.rechtspraak.nl/Organisatie/Rechtbanken/Noord-Holland/Nieuws/Pages/Straffen-tussen-10-en-20-jaar-voor-Purmerlandmoorden.aspx.
[15] Zie http://www.blikopnieuws.nl/2013/om-eist-10-jaar-en-tbs-wegens-doodslag-vriendin en http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2013:9145.

de historische gegevens van een in de verlate auto achtergelaten telefoon en in 2014 veroordeeld voor poging doodslag.[16]

Andere voorbeelden van recente uitspraken over levensdelicten waarin historische telecomgegevens voor het bewijs zijn gebruikt zijn:

- Gerechtshof Arnhem-Leeuwarden 26 februari 2015, doodslag partner[17]
- Gerechtshof Den Haag 18 februari 2015, doodslag ex-partner[18]
- Rechtbank Limburg 2 februari 2015, medeplegen moord[19]
- Rechtbank Limburg 27 januari 2015, 24 jaar gevangenisstraf voor martelmoord Maastricht[20]
- Hof Den Bosch 6 oktober 2014, doodslag op schoonzoon[21]
- Rechtbank Oost-Brabant 19 september 2014, poging doodslag[22]
- Rechtbank Oost-Brabant 28 juli 2014, poging doodslag door schietpartij[23]
- Gerechtshof 's-Hertogenbosch 28 mei 2014, poging doodslag op moeder[24]
- Rechtbank Rotterdam 28 mei 2014, moord voor levensverzekering[25]
- Rechtbank Rotterdam 21 mei 2014, doodslag met hakbijl en wegmaken lijk[26]
- Rechtbank Den Haag 2 mei 2014, doodslag in woning[27]
- Rechtbank Midden-Nederland 17 december 2013, moord in Almere[28]
- Rechtbank Den Haag 9 december 2013, doodslag op Haagse Rinus[29]
- Rechtbank Noord-Nederland 24 oktober 2013, moord in opdracht in Marum[30]
- Rechtbank Gelderland 19 september 2013, doodslag[31]
- Rechtbank Noord-Nederland 26 augustus 2013, doodslag bij woningoverval[32]
- Gerechtshof Den Haag 28 mei 2013, poging doodslag[33]
- Rechtbank Noord-Nederland 24 januari 2013, doodslag en wegmaken lijk[34]
- Rechtbank Utrecht 30 januari 2012, moord[35]

---

[16] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2014:8397.
[17] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHARL:2015:1384.
[18] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHDHA:2015:282.
[19] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBLIM:2015:789.
[20] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBLIM:2015:573.
[21] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHSHE:2014:4029.
[22] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBOBR:2014:5416.
[23] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBOBR:2014:4443.
[24] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHSHE:2014:1530.
[25] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBROT:2014:4364.
[26] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBROT:2014:4033.
[27] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2014:5510.
[28] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBMNE:2013:7281.
[29] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2013:18647.
[30] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBNNE:2013:6444.
[31] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBGEL:2013:3149.
[32] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBNNE:2013:5096.
[33] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHDHA:2013:CA2310.
[34] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBNNE:2013:BY9376.
[35] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBUTR:2012:BV2134.

Woningovervallen met geweld

Woningoverval waarbij bewoonster uit het raam wordt geduwd.
Op 9 september 2014 veroordeelt het gerechtshof Den Haag een man voor het met anderen plegen van een woningoverval tegen een gezin met een kind van drie jaar oud. De daders hebben de vrouwelijke bewoonster vanaf de eerste verdieping van de woning uit een geopend raam geduwd. Hierdoor is zij naar beneden gevallen en heeft zij zwaar lichamelijk letsel opgelopen. Zij heeft vier dagen in coma op de intensive care gelegen. Historische telefoongegevens waren voor de opsporing van de daders van groot belang en worden door het gerechtshof ook voor het bewijs gebruikt. [36]

Woningoverval Utrecht.
In juni 2014 veroordeelt de rechtbank Midden-Nederland een minderjarige dader voor een gewelddadige woningoverval op een hoogbejaarde man. De rechtbank gebruikt tot het bewijs onder meer de omstandigheid dat uit de historische gegevens van de telefoon van de dader blijkt dat hij in de nacht van de overval heeft gebeld via een telefoonmast in de nabije omgeving van de overvallen woning.[37]

Woningoverval Nieuw Heeten.
In december 2013 veroordeelt de Rechtbank Overijssel een man voor een gewelddadige overval op een woning in Nieuw Heeten.[38] De man is een woning binnengedrongen, heeft daar een meisje van vijftien bedreigd met verkrachting en de dood, en is daarna weggegaan met zijn buit – waaronder een mobiele telefoon. Aan de hand van de mastgegevens van de gestolen telefoon kan worden vastgesteld welke route de dader na de overval heeft afgelegd. Die route kan nauwkeurig worden gematcht met de route van een door verdachte gehuurde auto. Voor deze overval en enkele inbraken krijgt de dader een gevangenisstraf van 42 maanden.

Andere voorbeelden van recente uitspraken over woningovervallen waarin historische telecomgegevens voor het bewijs zijn gebruikt zijn:

- Gerechtshof Arnhem-Leeuwarden 19 februari 2015, woningoverval waarbij 72-jarige bewoonster overlijdt[39]
- Rechtbank Den Haag 24 december 2014, woningoverval waarbij 73 jarige bewoner geboeid wordt achtergelaten[40]
- Gerechtshof Amsterdam 11 november 2014, woningovervallen en overval op coffeeshop[41]
- Rechtbank Noord-Nederland 28 oktober 2014, woningoverval met geweld tegen een terminaal zieke, oudere man[42]

---

[36] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHDHA:2014:2943.
[37] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBMNE:2014:3380, r.o. 4.3.1.2.
[38] Zie . http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBOVE:2013:3196.
[39] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHARL:2015:1163 en eerder het vonnis van de rechtbank in deze zaak: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBOVE:2014:3946.
[40] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2014:16227.
[41] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHAMS:2014:4768.
[42] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBNNE:2014:5295.

- Rechtbank Zeeland-West-Brabant 1 september 2014, woningoverval waarbij een oudere man een klaplong en gebroken ribben oploopt[43]
- Gerechtshof Amsterdam 29 juli 2014, poging woningoverval met geweld[44]
- Gerechtshof Arnhem-Leeuwarden 8 juli 2014, woningoverval waarbij bewoner wordt neergestoken[45]
- Rechtbank Midden-Nederland 5 juni 2014, woningoverval met geweld bij hoogbejaarde man[46]
- Rechtbank Gelderland 9 april 2014, woningoverval met geweld[47]
- Rechtbank Noord-Holland 20 februari 2014, woningoverval waarbij gezin met twee jonge kinderen is vastgebonden met tie-wraps en is bedreigd met een vuurwapen[48]
- Gerechtshof Arnhem-Leeuwarden 27 juni 2013, woningoverval waarbij het slachtoffer is verkracht en zwaar gewond is geraakt na het tot ontploffing brengen van een vuurwerkbom[49]

Afpersing, diefstal met geweld

Bedreiging en afpersing motorclub Pegasus.
Op 13 februari 2015 veroordeelt de rechtbank Den Haag meerdere leden van de Trailer Trash Travellers voor afpersing met geweld van leden van de motorclub Pegasus.[50] Welke leden van de Trailer Trash Travellers aanwezig waren tijdens de afpersing werd in het onderzoek vastgesteld aan de hand van hun historische telefoongegevens. Deze worden door de rechtbank ook gebruikt voor het bewijs.

TBS voor neersteken slachtoffer bij scooterdiefstal.
Op 6 augustus 2014 veroordeelt de rechtbank Den Haag een man tot zeven jaar gevangenisstraf en TBS voor het neersteken van een man wiens scooter hij wil stelen.[51] De historische telefoongegevens van de dader, waaruit zijn aanwezigheid op de plaats delict blijkt, worden voor de opsporing en het bewijs gebruikt.

Overvaller geldtransporten.
Op 14 oktober 2014 veroordeelt het Gerechtshof Arnhem-Leeuwarden een man voor betrokkenheid bij overvallen op verschillende geldtransporten tot acht jaar gevangenisstraf.[52] Historische telefoongegevens zijn belangrijk geweest voor de opsporing en worden voor het bewijs gebruikt. Uit die gegevens is onder meer de

---

[43] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBZWB:2014:6065 en http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBZWB:2014:6066. .
[44] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHAMS:2014:3010.
[45] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHARL:2014:5426.
[46] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBMNE:2014:3380.
[47] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBGEL:2014:2408 en http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBGEL:2014:2410.
[48] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBNHO:2014:1410.
[49] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHARL:2013:4617.
[50] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2015:1460.
[51] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2014:9700.
[52] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHARL:2014:7846.

aanwezigheid van de verdachte bij de overvallen gebleken en zijn contacten met een chauffeur van een van de geldtransporten.

Week durende gijzeling van een achttienjarige jongen.
Op 20 augustus 2012 veroordeelt de rechtbank Utrecht verschillende verdachten voor de gijzeling van een achttienjarige jongen.[53] De daders eisten van zijn vader een losgeld van miljoenen euro's. De daders hebben hun slachtoffer, zo constateert de rechtbank, onder mensonterende omstandigheden een week lang geboeid en geblinddoekt vastgehouden. Hij kan bevrijd worden door een onderzoek waarin historische telefoongegevens een doorslaggevende rol spelen. Deze worden ook in het vonnis voor het bewijs gebruikt.

Andere voorbeelden van recente uitspraken over afpersing, afdreiging of diefstal met geweld waarin historische telecomgegevens voor het bewijs zijn gebruikt zijn:

- Hoge Raad 16 december 2014, beroving met vuurwapen[54]
- Gerechtshof Den Haag 1 oktober 2014, overval met grof geweld op juwelier[55]
- Gerechtshof 's-Hertogenbosch 19 juni 2014, autodiefstal met geweld[56]
- Gerechtshof Amsterdam 1 mei 2014, overval op supermarkt[57]
- Rechtbank Gelderland 4 februari 2014, afdreiging[58]
- Rechtbank Midden-Nederland 31 oktober 2013, overval op juwelier[59]

<u>Zedendelicten</u>

Online kindermisbruiker.
Op 12 februari 2015 veroordeelt de rechtbank Amsterdam een man tot een meerjarige gevangenisstraf omdat hij gedurende een periode van meer dan zeven jaren met misleiding en bedreiging met zeer grote regelmaat jonge kinderen er toe heeft gebracht voor de webcam seksuele poses aan te nemen en seksuele handelingen te verrichten.[60] Daarvan heeft de man opnames gemaakt die hij bewaarde en verspreidde, ook naar andere kinderen. De rechtbank noemt de man (r.o. 8.4) 'manipulatief en in veel gevallen dwingend, grof en soms zelfs agressief in zijn benadering van de (soms zeer) jonge slachtoffers'. De rechtbank beschrijft ook hoe de man, die voor zijn contacten een hotmail-adres op naam van een ander gebruikte, is opgespoord (r.o. 4.1): onderzoek naar het IP-adres gebruikt door verdachte in dreigende chats met een kind van twaalf leidde naar zijn woning, waar bij een doorzoeking in zijn computer veel belastend materiaal werd gevonden. De rechtbank schrijft in het vonnis (r.o. 8.4):

> "De enkele filmfragmenten die de rechtbank ter terechtzitting kort heeft besproken zijn echter ronduit schokkend te noemen en geven een kort inzicht in de afschuwelijke wereld van de kinderporno-industrie. Hier benadrukt de rechtbank daarom dat het verwerven van kinderporno, relatief gemakkelijk

[53] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBUTR:2012:BX5060.
[54] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:HR:2014:3634.
[55] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHDHA:2014:3283.
[56] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHSHE:2014:1817.
[57] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHAMS:2014:3605.
[58] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBGEL:2014:849.
[59] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBMNE:2013:5412.
[60] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2015:673.

vanachter een computer thuis en zogenaamd op afstand, krachtig moet worden bestreden.”

De eerste aangifte tegen deze dader werd gedaan meer dan een maand na de laatste chats tussen de dader en dat slachtoffer, omdat de moeder van het slachtoffer deze chats pas na enige tijd ontdekte. Het kunnen vorderen van IP-adressen ouder dan een maand was dus een noodzakelijke voorwaarde voor dit onderzoek.

Verkrachting.

Bij zedendelicten is vaak sprake van een gebrek aan getuigen. Het is dan het woord van de aangeefster tegen het woord van de verdachte, en er is een groot belang bij objectieve gegevens om te kunnen controleren wie de waarheid spreekt. Telecomgegevens kunnen soms die rol spelen. Zo veroordeelt de rechtbank Midden-Nederland in december 2014 een man voor een verkrachting.[61] Zijn verklaring dat er alleen sprake was van vrijwillige seks vindt de rechtbank ongeloofwaardig omdat uit de opgevraagde belgegevens van het slachtoffer blijkt dat zij, zoals zij wel verklaart en hij niet, rondom de verkrachting telefonisch contact heeft gehad met een ongeruste vriendin.

Mensenhandel zwakbegaafde vrouw.

In februari 2014 veroordeelt de rechtbank Gelderland een man tot drie jaar gevangenisstraf voor mensenhandel.[62] Hij heeft een zwakbegaafde, drugsverslaafde jonge vrouw in seksclubs door heel Nederland laten werken, hetgeen met name is vastgesteld aan de hand van de historische gegevens van de telefoons van zowel het slachtoffer als de dader.[63] Doordat die gegevens over een langere tijd konden worden opgevraagd, kan worden vastgesteld en bewezen dat de mensenhandel zich over een langere periode heeft afgespeeld. Door historische gegevens van verschillende telefoons met elkaar te combineren kan de rechtbank vaststellen welke telefoons door verdachte zijn gebruikt.

Misbruik gedwongen minderjarige prostituee.

In januari 2014 meldde zich een minderjarige vrouw die gedwongen werd tot prostitutie. Zij vertelde misbruikt te zijn door een man die bij de eerste afspraak had afgezien van seks omdat zij hem huilend had verteld minderjarig te zijn en gedwongen te worden om seks te hebben met klanten. Omdat de man zijn vooruitbetaalde geld niet terug had gekregen van haar pooier, heeft hij haar op een tweede afspraak wel misbruikt. Deze ‘klant’ kon worden geïdentificeerd mede aan de hand van de historische gegevens van de telefoon waarmee hij had gereageerd op de advertentie waarin het meisje werd aangeboden en werd in februari 2015 veroordeeld.[64]

Ook de man die het meisje in de prostitutie had bracht en daarvan profiteerde werd veroordeeld. Hij werd opgespoord door onderzoek te doen naar het IP-adres dat was gebruikt om seksadvertenties voor het meisje te plaatsen, en naar de historische gegevens van het in die advertenties vermelde telefoonnummer.[65]

---

[61] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBMNE:2014:6502.
[62] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBGEL:2014:594.
[63] Zie met name r.o. 3 ten aanzien van feit 2 en slachtoffer 2.
[64] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBMNE:2015:745 m.n. r.o. 4.3.1.4.
[65] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBMNE:2015:742.

Maandenlange verkrachtingen vermiste vrouw.
In februari 2012 wordt een vermiste vrouw aangetroffen in een woning. Zij is getraceerd aan de hand van haar historische telefoongegevens. Het blijkt dat zij maandenlang van haar vrijheid is beroofd, vernederd, ernstig mishandeld, gedwongen tot het nemen van drugs, alcohol en medicijnen en vrijwel dagelijks verkracht door twee mannen. De rechtbank spreekt van 'één van de meest vreselijke wijzen van vrijheidsberoving die men zich kan voorstellen' en 'een script van een horror-film [dat] gedurende een periode van drie en een halve maand de realiteit is geweest voor een kwetsbare, dove vrouw'. In maart 2013 worden de twee daders veroordeeld tot zeven en negen jaar gevangenisstraf en (beiden) TBS met dwangverpleging.[66]

Mensenhandelaars Amsterdam.
In juni 2013 veroordeelt de rechtbank Amsterdam een man tot negen jaar gevangenisstraf omdat hij vier vrouwen heeft gedwongen tot prostitutie. De rechtbank concludeert dat de man zijn slachtoffers op een gruwelijke wijze heeft uitgebuit en heeft getekend voor het leven. De resultaten van het historische telecomonderzoek bevestigen de verklaringen van de slachtoffers en worden voor het bewijs gebruikt.[67]

In dezelfde maand worden in Amsterdam twee andere mannen veroordeeld tot gevangenisstraffen van vier jaar omdat zij een slachtoffer volgens de rechtbank gedurende vijf maanden hebben 'mishandeld, verkracht en bedreigd wanneer het hen uitkwam'. Ook bij deze daders worden de resultaten van het historische telecomonderzoek voor het bewijs gebruikt.[68]

En ook op 13 maart 2015 veroordeelt de rechtbank Amsterdam een man voor mensenhandel – waarbij gepoogd werd een meisje van veertien jaar oud in de prostitutie te brengen - met gebruikmaking van historische telecomgegevens.[69]

Uit onderzoek blijkt ook dat historische telecomgegevens van groot belang zijn voor de aanpak van mensenhandel.[70]

Belaging (stalking)

Stalking zaken hebben een grote impact op slachtoffers en eindigen, wanneer deze zaken niet in een vroeg stadium worden aangepakt, meer dan eens in een daadwerkelijk fysiek bedreigende situatie voor het slachtoffer.
Voor het aantonen van met name het bij herhaling lastig gevallen worden via de telefoon (gesprekken, SMS-berichten, etc.) zijn historische verkeersgegevens over een langere termijn onontbeerlijk. Ook voor het achterhalen van de herkomst van vaak anonieme mails of, zoals we steeds vaker zien, ongewenste aanpassingen op pagina's van social

[66] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBMNE:2013:BZ4143 en http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBMNE:2013:BZ4175.
[67] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2013:CA3399.
[68] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2013:CA3415 en http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2013:CA3711.
[69] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2015:1424.
[70] Zie bijv. https://technologyandtrafficking.usc.edu/the-rise-of-mobile-phones-in-human-trafficking/.

media zoals Facebook, is verder onderzoek naar uit digitaal onderzoek gebleken IP-adressen onontbeerlijk. Historische telefoon- en internetgegevens zijn daarbij vaak het enige middel.
Belaging wordt vaak berecht door de politierechter en de vonnissen worden veelal niet gepubliceerd.

Voorbeelden van recente wel gepubliceerde uitspraken over belaging waaruit het belang van historische telecomgegevens blijkt, zijn:

- Rechtbank Noord-Holland 13 augustus 2014[71]
- Rechtbank Limburg 9 juli 2014[72]
- Gerechtshof Arnhem-Leeuwarden 10 februari 2014[73]
- Rechtbank Midden-Nederland 9 juli 2013[74]`

Andere inbreuken op de privacy

De opsporingspraktijk wordt in toenemende mate geconfronteerd met andere inbreuken op de privacy door burgers onderling, zoals het illegaal plaatsen van bakens onder auto's. Dat kan bijvoorbeeld tot doel hebben diefstal (al dan niet van drugs) of moord voor te bereiden.[75] Als een illegaal baken wordt ontdekt door een burger voordat het misdrijf waartoe dat baken diende is uitgevoerd, zijn de historische gegevens van de Sim-kaart in het baken vaak het meest directe, en soms het enige aanknopingspunt voor onderzoek.[76] Gelet op de vermoedelijk slechte bedoelingen van de plaatser van het baken is er een groot belang om zo snel mogelijk duidelijkheid te krijgen over diens identiteit teneinde het voorgenomen misdrijf te voorkomen. Niet ingrijpen en het laten functioneren van het baken om daarmee zicht te krijgen op toekomstige telecomgegevens levert risico op en is daarom doorgaans geen optie.

Cybercrime

Bij het plegen van cybercrime wordt vaak gebruik gemaakt van afschermingstechnieken, waardoor onderzoek naar een gebruikt IP-adres niet direct leidt tot de werkelijke gebruiker maar naar een ander IP-adres, vaak uit een ander land. Hierdoor stuit men bij de opsporing van cybercrime vaak op IP-adressen over de hele wereld en zijn rechtshulpverzoeken noodzakelijk voor ieder IP-adres. De tijd die verstrijkt voordat vervolgens nader onderzoek kan worden gedaan naar het volgende IP-adres beslaat doorgaans maanden. De informatie moet bij het andere land worden opgevraagd, de rechtsgang daar moet worden gevolgd en de resultaten ervan moeten worden teruggekoppeld en onderzocht. Daar gaat langere tijd overheen. Het vergt vervolgens een

---

[71] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBNHO:2014:7824, met name r.o. 4.2.3.
[72] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBLIM:2014:6091, met name r.o. 4.3.
[73] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHARL:2014:868.
[74] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBMNE:2013:2719, met name r.o. 4, feit 4.
[75] Zie bijv. http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHARN:2012:BX7827 en http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBROT:2012:BV2735 (twee zaken betreffende moorden die vooraf werden gegaan door het plaatsen van een illegaal baken onder de auto's van de slachtoffers).
[76] Zie bijv. http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBNNE:2014:2018.

complexe analyse van de resultaten van alle stappen om tot het herleiden van het primaire IP-adres te komen.

Nederland is een belangrijk internet knooppunt, veel internationaal internetverkeer gaat door de Nederlandse infrastructuur. Met een beperking of afschaffing van de bewaartermijn zal het zeer lastig zijn om in opsporingsonderzoeken met een internationaal karakter, wat steeds vaker voorkomt, nog nader onderzoek te kunnen doen naar de opvolgende IP-adressen die uit dat onderzoek naar voren komen. Het zal in dat geval voor Nederland ook zeer lastig worden om te voldoen aan internationale verplichtingen, voortvloeiend uit rechtshulpverdragen, om vragen vanuit het buitenland, naar informatie over IP-adressen, te beantwoorden. Nu Nederland een vooraanstaande positie heeft in de infrastructuur voor het internet, zal dat veel internationale cybercrime zaken kunnen raken.

Op internet en in de hacker community is de ervaring, betrouwbaarheid en kennis van een hacker vaak te ontlenen aan zijn “nickname”. Dat is de naam die op internet wordt gebruikt en in veruit de meeste gevallen niet de werkelijke naam van de betrokkene betreft of tot hem/haar te herleiden is. Waar in de fysieke wereld bij het plegen van strafbare feiten sporen kunnen worden achtergelaten doordat je zichtbaar bent voor een getuige of dat je vingerafdrukken of DNA achterlaat, laat je in de digitale wereld meestal alleen IP-sporen na, al dan niet via de zogenaamde “nickname”. Anders dan in de fysieke wereld is een IP-spoor dan ook vaak het enige aanknopingspunt. Indien de historische gegevens niet of slechts gedurende kortere tijd, beschikbaar zijn, zullen veel van dit soort zaken niet kunnen worden opgespoord nu van het enige aanknopingspunt (IP-adres) de historische verkeersgegevens en/of gebruiksgegevens niet meer te achterhalen zijn.

Voorbeelden van vonnissen waaruit het belang van historische telecomgegevens voor de opsporing van cybercrime blijkt, zijn de volgende:

Hack ziekenhuis.
Op 17 december 2014 veroordeelt de rechtbank in Den Haag een man voor het hacken van een server van het Groene Hart ziekenhuis en voor bezit van kinderpornografisch materiaal.[77] Verdachte heeft het hacken van het netwerk van het ziekenhuis bekend. Aan de identificatie van verdachte wordt in het vonnis dan ook niet veel aandacht besteed. Uit de bewijsoverwegingen kan echter wel worden opgemaakt dat het spoor naar deze verdachte gevonden werd doordat de man bij het uploaden van malware op de server van het ziekenhuis niet zijn geanonimiseerde Zweedse internetverbinding kon gebruiken, maar een ander, Nederlands, IP-adres heeft gebruikt. Uitsluitend door het gebruik van dit IP-adres kon verdachte worden geïdentificeerd. Voor het tweede deel van de hack, waarbij een enorme hoeveelheid medische persoonsgegevens en volledige medische dossiers zijn buit gemaakt, is verdachte uiteindelijk vrijgesproken. Belangrijkste reden daarvoor is dat dit deel van de hack heeft plaatsgevonden via een IP-adres van een anonimiseringsdienst, dat leidt tot een bedrijf in Zweden dat - doelbewust - geen gegevens bewaart. Hierdoor zijn geen historische gegevens betreffende dit IP-adres verkregen en blijft het werkelijk gebruikte IP-adres verborgen. Door het ontbreken van

[77] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2014:15611

deze gegevens is dit belangrijke deel van de hack, waarbij de medische gegevens van meer dan 500.000 Nederlandse patiënten zijn gestolen, onopgelost gebleven. Deze zaak illustreert duidelijk hoe de (verplichte) beschikbaarheid van telecomgegevens beslissend kan zijn voor succes in de opsporing, juist ook van misdrijven waarmee grootschalig en ernstig inbreuk wordt gemaakt op de privacy van slachtoffers.

DDOS-aanval op een Nederlandse bank.
Op 2 september 2014 veroordeelt[78] de rechtbank Zeeland-West-Brabant een minderjarige verdachte voor een "denial of service" (DOS) aanval op een Nederlandse Bank. Door de aanval konden klanten van de bank geen gebruik maken van internetbankieren, iDeal en mobiel bankieren. Verdachte heeft deze aanval gepleegd gedurende een periode in april 2013 waarin door anderen de websites en internetbankieren van vele Nederlandse banken en enkele andere grote websites zware Distributed Denial of Service (DDOS)-aanvallen te verduren kregen en meermalen uren onbereikbaar waren. Verdachte kon alleen worden opgespoord door de gegevens van het IP-adres dat bij de aanval naar voren kwam. Dit is uitdrukkelijk in de overwegingen van de rechtbank opgenomen.

Hacking, oplichting en phishing.
Op 17 februari 2015 veroordeelt de rechtbank Midden-Nederland verdachte voor hacking en het vervolgens oplichten van (klanten van) verschillende webwinkels en van een bank.[79] De verdachte was betrokken bij een criminele organisatie die zich gedurende lange tijd bezighield met phishing fraude. De organisatie verstuurde een phishing e-mail bijvoorbeeld uit naam van een bekende webwinkel of bank met daarin een link naar een nagemaakte inlogpagina van die webwinkel of bank. Nadat de lezer op deze neppagina zijn inloggegevens had ingevoerd, kon de organisatie met die inloggegevens op de echte pagina van de webwinkel bestellingen plaatsen of inloggen op internetbankieren. Er werden op deze manier onder andere telefoons, tablets, laptops en camera's besteld. Vervolgens werden de afleveradressen van de bestaande klanten gewijzigd. De gewijzigde adressen werden doorgeven aan postbezorgers, die tevens deel uitmaakten van de criminele organisatie. De postbezorgers tekenden indien nodig voor ontvangst en hielden de pakketten achter. Er werd nooit voor de bestelde goederen betaald.
Onderzoek naar gebruikte IP-adressen en mailadressen is een cruciaal onderdeel van het onderzoek geweest, tezamen met historische telefoongegevens en uiteindelijk onderzoek aan de computers. Het is vooral een combinatie van gegevens die tot identificatie van deze verdachte heeft geleid. De rechtbank besteedt uitgebreid aandacht aan deze gegevens in de bewijsoverwegingen.

Phishing en criminele organisatie.
Op 21 oktober 2013 veroordeelt[80] de rechtbank Noord-Holland meerdere verdachten voor het op grote schaal en gedurende langere periode oplichten van rekeninghouders van verschillende banken door midden van phishing en witwassen. Door middel van phishing zijn aanzienlijke geldbedragen van een groot aantal – kennelijk op hun kwetsbaarheid en goedgelovigheid geselecteerde – slachtoffers weggesluisd en tijdelijk

[78] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBZWB:2014:6659
[79] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBMNE:2015:922.
[80] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBNHO:2013:9735

geparkeerd op rekeningen van begunstigden, met de bedoeling om de gelden direct van die rekening op te nemen, zodat deze niet langer traceerbaar zouden zijn. In de bewijsconstructie besteedt de rechtbank aandacht aan historische verkeersgegevens en locatiegegevens.

Fraude

Ook voor de bestrijding van fraude is het gebruik van historische telecomgegevens vaak nuttig en soms noodzakelijk om resultaat te kunnen boeken. In november 2014 werden bijvoorbeeld meerdere verdachten veroordeeld voor grootschalige kinderopvangtoeslagfraude waarmee de Belastingdienst voor miljoenen euro's werd opgelicht.[81] In het onderzoek kon worden vastgesteld dat 143 toeslagaanvragen op naam van anderen waren ingediend vanaf zeven IP-adressen. Doordat kon worden vastgesteld bij wie die IP- adressen in gebruik waren tijdens het indienen van de aanvragen kon de criminele organisatie achter deze fraude worden aangehouden. In het onderzoek werd vermoed dat de fraudeurs verantwoordelijk waren voor nog honderden andere valse aanvragen, waarmee ook voor miljoenen was gefraudeerd. Omdat van die aanvragen de bewaartermijn was verstreken en geen gegevens meer gevorderd konden worden over de gebruikte IP-adressen, konden deze gevallen echter niet worden bewezen.

Zie verder bijvoorbeeld:
- Rechtbank Zeeland-West-Brabant 9 februari 2015, criminele organisatie vervalsers[82]
- Rechtbank Den Haag 16 mei 2014, omzetbelastingfraude[83]

Drugscriminaliteit

Bij het opsporen van criminele organisaties die zich bezig houden met drugscriminaliteit kan door middel van historische telecomgegevens belangrijke informatie en bewijs worden verkregen over de contacten tussen de verschillende leden van de organisatie en andere betrokkenen bij hun misdrijven. Voorbeelden van recente uitspraken waaruit dit blijkt zijn:
- Rechtbank Noord-Holland 27 februari 2015, cocaïne smokkel via Schiphol[84]
- Rechtbank Gelderland 17 februari 2015, grootschalige hennepteelt [85]
- Rechtbank Noord-Holland 8 december 2014, cocaïne smokkel via Antwerpen[86]
- Gerechtshof Amsterdam 19 september 2014, cocaïne smokkel via Schiphol[87]
- Rechtbank Noord-Holland 8 september 2014, 7 jaar gevangenisstraf voor 12 drugstransporten vanuit Argentinië, Brazilië en Suriname naar Nederland [88]

---

[81] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2014:8430.
[82] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBZWB:2015:836.
[83] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2014:6048.
[84] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBNHO:2015:1602.
[85] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBGEL:2015:985.
[86] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBNHO:2014:12529.
[87] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHAMS:2014:3893.
[88] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBNHO:2014:8607.

Bedreiging en ernstige verstoring van de openbare orde

In gevallen van bedreiging, afdreiging of afpersing via telefoon of internet door anonieme personen, vormen historische telecomgegevens vaak het meest concrete en soms zelfs het enige aanknopingspunt voor onderzoek. In de jurisprudentie zijn verschillende vonnissen te vinden over bedreiging en afdreiging waaruit blijkt dat de daders zijn gevonden aan de hand van deze gegevens. Daaronder bevinden zich ook zaken met grote impact op de Nederlandse samenleving en de openbare orde, zoals de bedreiging van politici en aankondigingen van schietpartijen op scholen die hebben geleid tot grote onrust en ingrijpende openbare orde maatregelen, waaronder ontruiming en politiebewaking van de betreffende scholen.

Dreiging schoolshooting Leiden.
Op 19 november 2013 veroordeelt[89] de rechtbank Den Haag een man voor bedreiging van een leraar en studenten van een Leidse school door via een internetforum te dreigen met een zogenaamde schoolshooting. De man had in twee dreigende berichten op de internetwebsite 4chan een schietpartij op een school in Leiden aangekondigd, waarbij een leraar en meerdere leerlingen zouden worden neergeschoten. De politie, de burgemeester en de schooldirecties hebben de berichten zodanig serieus genomen dat de scholen op maandag 22 april 2013 gesloten zijn geweest, mede omdat er in het verleden schietpartijen op scholen elders in de wereld hebben plaatsgevonden met gewonden en dodelijke slachtoffers, waaraan door de media veel aandacht is besteed. Bij een aantal van deze schietpartijen was ook sprake van een anonieme aankondiging via internet vooraf. In de dagen na de bedreigingen werden de scholen grootschalig beveiligd met politie-eenheden. Tevens werd het onderzoek van de zaak verricht door een grootschalig onderzoeksteam, om zo spoedig mogelijk te achterhalen wie het bericht geplaatst had en om zodoende de dreiging weg te kunnen nemen, met de inzet van veel politiecapaciteit. Verdachte is opgespoord aan de hand van het gebruikte IP-adres in beide berichten.

Voorbeelden van andere recente uitspraken, waarin historische telecomgegevens noodzakelijk zijn geweest voor de opsporing en het bewijs van bedreigingen en ernstige verstoringen van de openbare orde, zijn:

- Rechtbank Overijssel 29 april 2014, bommeldingen per email waarna ontruiming ROC Almelo[90]
- Gerechtshof ’s-Gravenhage 14 oktober 2013, bedreiging school Den Haag via internet[91]
- Rechtbank Breda 9 november 2010, bedreiging met ‘schoolshooting’ in Breda[92]

[89] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2013:15617
[90] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBOVE:2014:2282. Zie ook http://www.tubantia.nl/regio/almelo/almelose-leerlingen-op-straat-na-bommelding-1.3849335.
[91] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHDHA:2013:3871. Een duidelijker beschrijving van de wijze waarop de dader is gevonden aan de hand van historische telecomgegevens is te vinden in een eerdere uitspraak in deze zaak, namelijk http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHSGR:2011:BP7080.
[92] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBBRE:2010:BO3363.

- Gerechtshof Den Haag 23 maart 2010, bedreiging landelijk politicus via email[93]

Terroristische misdrijven

Terroristische misdrijven komen, gelukkig, minder vaak voor dan ‘commune’ misdrijven, maar als zij plaatsvinden is het van groot belang om daders en medeplichtigen op te sporen, het gevaar te beëindigen en herhaling te voorkomen. De ervaringen met terroristische aanslagen in het buitenland wijzen uit dat de beschikbaarheid van telecomgegevens daarvoor van groot belang is.

In Frankrijk werd Mohamed Merah, die in maart 2012 binnen twee weken zeven mensen dood schoot, getraceerd aan de hand van de historische gegevens van zijn internetcontact met zijn eerste slachtoffer.[94] Duitsland heeft daarna gemeld dat door het afschaffen van de bewaarplicht het bij hen niet mogelijk was geweest om Merah op zo’n wijze te traceren.[95]

Dat telecomgegevens belangrijk zijn voor terrorismebestrijding, blijkt ook uit het politieoptreden na de aanslag op het tijdschrift *Charlie Hebdo* in Parijs. Banden tussen de aanslagplegers werden vastgesteld op basis van telefonische contacten en de locatiegegevens van hun telefoongebruik.[96] Dat Hayat Boumeddiene, de enige nog levende verdachte, naar Syrië is gereisd, bleek uit haar telefoongegevens.[97] Verdachten van medeplichtigheid konden worden geïdentificeerd en aangehouden mede op basis van historisch telecomonderzoek.[98]

In het Verenigd Koninkrijk concludeerde de regering dat telecomgegevens een significante rol hebben gespeeld in elke grote terrorismezaak van de afgelopen tien jaar, waaronder bijvoorbeeld de aanval op het vliegveld van Glasgow in 2007.[99]

Het Speciaal Tribunaal voor Libanon heeft de verdachten van de bomaanslag op Hariri in 2005 opgespoord dank zij een zeer uitgebreid onderzoek naar historische telecomgegevens dat uitvoerig wordt beschreven in de aanklacht (*indictment*) tegen Ayyash en anderen.[100]

---

[93] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHSGR:2010:BN6708.
[94] Zie https://cyberarms.wordpress.com/2012/03/23/ip-address-leads-police-to-french-terrorist/.
[95] Zie http://www.welt.de/politik/deutschland/article13942623/Bei-uns-haette-man-Mohamed-Merah-nicht-ermittelt.html.
[96] Zie bijv. http://nos.nl/artikel/2019842-daders-hadden-uur-voor-aanslagen-parijs-contact.html en http://www.cbsnews.com/news/paris-terror-ahmedy-coulibaly-cherif-kouachi-spoke-hour-before-attacks/. .
[97] Zie http://www.hln.be/hln/nl/32542/Aanslag-Charlie-Hebdo/article/detail/2180342/2015/01/13/Hoe-de-veiligheidsdiensten-Hayat-Boumeddiene-lieten-lopen.dhtml.
[98] Zie http://www.smh.com.au/world/paris-terror-attacks-four-held-over-links-to-grocery-store-gunman-amedy-coulibaly-20150310-13zk6u.html.
[99] Zie https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/379775/IP_Resolution_IA.pdf en https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228726/7586.pdf, p. 9.
[100] Beschikbaar op http://www.stl-tsl.org/.

In Spanje waren telecomgegevens van groot belang voor het onderzoek naar de bomaanslagen in Madrid in 2004.[101]

Ook in Nederlandse terrorisme-onderzoeken worden vrijwel altijd historische telecomgegevens gevorderd om contacten, activiteiten en verplaatsingen van verdachten vast te stellen.

Overige misdrijven

Ook bij vele andere soorten misdrijven worden historische telecomgegevens gebruikt om effectief te kunnen opsporen, zoals mensensmokkel, geweldsmisdrijven, woninginbraken en andere (georganiseerde, beroepsmatige of grootschalige) diefstallen.

Zie verder bijvoorbeeld:
- Rechtbank Oost-Brabant 3 maart 2015, georganiseerde ladingdiefstallen[102]
- Rechtbank Gelderland 27 februari 2015, diefstallen van honderden schapen[103]
- Rechtbank Den Haag 11 februari 2015, meerdere diefstallen[104]
- Rechtbank Overijssel 29 december 2014, inbraken[105]
- Rechtbank Gelderland 8 december 2014, diefstal van militaire goederen[106]
- Rechtbank Noord-Nederland 27 november 2014, woninginbraken met autodiefstallen[107]
- Rechtbank Den Haag 14 oktober 2014, acht jaar gevangenisstraf voor verschillende geweldsmisdrijven[108]
- Gerechtshof Arnhem-Leeuwarden 2 oktober 2014, woninginbraken[109]
- Rechtbank Den Haag 13 augustus 2014, woninginbraken bij hulpbehoevende bejaarden met sleutelkastjes[110]
- Rechtbank Overijssel 4 maart 2014, mensensmokkel[111]
- Rechtbank Gelderland 19 februari 2014, woninginbraken[112]
- Rechtbank Noord-Holland 7 februari 2014, diefstal met bedreiging tegen 92 jarige bewoonster[113]

---

[101] Zie http://www.nytimes.com/2006/04/09/world/europe/09iht-spain.html ("Investigators working with [onderzoeksrechter] del Olmo say that practically all of the principal members of the group are now dead or in custody, and that they have unraveled most of what the group did in the days leading up to the attacks, largely through information gathered from phone records.").
[102] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBOBR:2015:1111.
[103] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBGEL:2015:1268 en http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBGEL:2015:1260 en http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBGEL:2015:1292.
[104] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2015:1322.
[105] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBOVE:2014:6925.
[106] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBGEL:2014:7575.
[107] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBNNE:2014:5872.
[108] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2014:12507.
[109] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHARL:2014:7617.
[110] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2014:16722.
[111] Zie bijv. http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBOVE:2014:1021. .
[112] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBGEL:2014:1084 en http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBGEL:2014:1088.
[113] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBNHO:2014:2500.

- Gerechtshof Amsterdam 20 januari 2014, groot aantal woninginbraken[114]

Telecomgegevens als ontlastend bewijs

Historische telecomgegevens kunnen niet alleen belastend bewijs, maar ook belangrijk ontlastend bewijs vormen. Zo sprak de rechtbank Den Haag in oktober 2014 een verdachte vrij van een poging tot uitlokking van moord.[115] Daarbij sloot de rechtbank een verklaring van een belangrijke belastende getuige uit van het bewijs omdat zij deze onbetrouwbaar achtte, onder meer omdat aan de hand van historische telefoongegevens is vastgesteld dat de getuige ter zitting heeft gelogen.[116] Na uitsluiting van de verklaringen van deze getuige bleef er onvoldoende bewijs over voor een veroordeling. Zo zijn er meer voorbeelden waarbij niet wordt vervolgd of vrijspraak volgt omdat uit historische telecomgegevens blijkt dat aangevers of getuigen niet de waarheid spreken.[117]
In februari 2015 werd bijvoorbeeld een verdachte vrijgesproken op Bonaire van de geruchtmakende dubbele moord in de zaak Country Garden omdat de rechter in die zaak constateerde dat een belangrijke belastende getuige 'wisselende verklaringen [had] afgelegd, die op onderdelen in strijd zijn met de telecomgegevens'.[118]

Meestal blijft de waarde van historische telecomgegevens als ontlastend bewijs echter buiten het zicht van het publiek omdat er geen zaak aan de rechter wordt voorgelegd als uit telecomgegevens blijkt dat een verklaring of aangifte onjuist is. Een voorbeeld daarvan: een buitenlandse vrouw doet in 2011 aangifte van uitbuiting. Zij zegt onder valse voorwendselen naar Nederland te zijn gehaald om in de prostitutie te werken en enige tijd onder dwang te zijn vastgehouden in Nederland. Door onderzoek te doen naar historische telecomgegevens konden van de aangeefster reisbewegingen en contacten worden vastgesteld die onverenigbaar waren met haar aangifte. Door verder te rechercheren op de informatie uit het telecomonderzoek konden getuigen worden gevonden en gehoord die bevestigden dat het verhaal van de aangeefster onjuist was. Het onderzoek wordt daarom stopgezet.

Tenslotte

Om meer inzicht te geven in de wijze waarop historische telecomgegevens gebruikt worden in de opsporing beschrijven wij – in aanvulling op de in dit rapport zelf genoemde voorbeelden – in een bijlage bij dit rapport van meerdere zaken in meer detail hoe historische telecomgegevens zijn gebruikt voor de opsporing of juist niet konden worden gebruikt.
Daarbij wordt onder meer aandacht besteed aan het (kinderporno)netwerk rond Robert M.

---

[114] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHAMS:2014:46.
[115] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2014:13131.
[116] Zie r.o. 3.1.4.
[117] Zie bijv. http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBROE:2012:BY0623. Zie ook http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHDHA:2015:282 (veroordeling van dader en verwerping van zijn beschuldiging tegen een ander mede op grond van de historische telecomgegevens van beiden).
[118] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:OGEABES:2015:4.

Hoofdstuk 3. Waarom het belang van de bewaarplicht niet becijferd kan worden

Ieder jaar opnieuw worden historische telecomgegevens in vele duizenden opsporingsonderzoeken gebruikt. Dat dat van groot belang is voor de opsporing, blijkt uit vele rechterlijke uitspraken die worden gepubliceerd op rechtspraak.nl, waaronder de tientallen voorbeelden genoemd in hoofdstuk 2 van dit rapport.

Het is echter een misverstand te denken dat alleen in die zaken historische telecomgegevens belangrijk zijn geweest. In de eerste plaats omdat lang niet alle rechterlijke uitspraken worden gepubliceerd. In de tweede plaats omdat gepubliceerde vonnissen lang niet altijd expliciet ingaan op het gebruik van historische telecomgegevens, ook als dat in het onderzoek van groot belang is geweest. En in de derde plaats omdat historische telecomgegevens niet alleen belangrijk zijn voor het verzamelen van bewijs Nederlandse strafzaken, maar ook voor het traceren en aanhouden van voortvluchtigen en het verlenen van rechtshulp aan andere landen. De resultaten daarvan zijn in Nederlandse vonnissen niet terug te vinden. Alle drie deze onderdelen worden hierna toegelicht.

Niet alle vonnissen worden gepubliceerd

Op rechtspraak.nl wordt maar een heel klein deel van alle rechterlijke uitspraken gepubliceerd. Van iedere 1000 vonnissen werden er in 2013 maar 26 gepubliceerd op rechtspraak.nl.[119] Rechtspraak.nl sprak zelf in januari 2014 nog van ‘maar een fractie van het totaal aantal uitspraken’ dat wordt gepubliceerd.[120] Deze cijfers zien op de rechtspraak als geheel (dus ook bestuursrecht, civiel recht, etc.) Welk percentage van de strafrechtelijke uitspraken wordt gepubliceerd is onbekend, maar duidelijk is in ieder geval dat ook van strafvonnissen de overgrote meerderheid niet wordt gepubliceerd.
Van de vonnissen over ernstige strafbare feiten worden er relatief meer gepubliceerd dan van vonnissen over bijvoorbeeld overtredingen. Ook van vonnissen over ernstige strafbare feiten wordt echter maar een kleine minderheid gepubliceerd. Om dat te illustreren kunnen we de periode nemen tussen 1 oktober 2009 en 30 september 2010. In dat jaar zijn er door de rechtbanken 62.165 vonnissen gewezen over gewelds- en vermogensdelicten.[121] Op rechtspraak.nl zijn 3064 strafrechtelijke vonnissen en beschikkingen van rechtbanken uit die periode gepubliceerd. Let wel: dit zijn niet alleen vonnissen maar ook beschikkingen (bijvoorbeeld betreffende wraking, beklagzaken en voorlopige hechtenis), en betreffende *alle* soorten misdrijven en overtredingen. Van de 62.165 vonnissen over gewelds- en vermogensdelicten in die genoemde twaalf maanden zijn er dus in ieder geval minder dan 3064 – dat is minder dan 5% - gepubliceerd.
Anders dan soms wordt gedacht, worden dus ook van ernstige strafbare feiten zeer vele uitspraken van de strafrechter niet gepubliceerd. Ook bij die uitspraken zijn er vele,

---

[119] Zie http://www.rechtspraak.nl/Organisatie/Publicaties-En-Brochures/Documents/kengetallen-2013.pdf, p. 26.
[120] Zie http://www.rechtspraak.nl/Organisatie/Rechtbanken/Gelderland/Nieuws/Pages/In2013minderGelderseuitsprakengepubliceerdopRechtspraaknl.aspx.
[121] Zie Algemene Rekenkamer, Prestaties in de strafrechtketen 2012, neergelegd in Kamerstukken II 2011/12, 33173, 1 en 2, p. 21.

onbekend voor het publiek, waarin historische telecomgegevens worden gebruikt voor het bewijs of worden vermeld vanwege hun belang voor het onderzoek.

Enkele voorbeelden van vonnissen over ernstige strafbare feiten die niet zijn gepubliceerd en waarin historische telecomgegevens een belangrijke rol spelen:

Liquidatie Albanees in Amsterdam.
Op 10 november 2014 werd een Albanese man veroordeeld tot vijftien jaar gevangenisstraf voor het liquideren van een andere Albanese man in Amsterdam in 2013. In het onderzoek was aan de hand van historische telecomgegevens geconstateerd dat de dader een prepaidtelefoon had gebruikt na aankomst in Amsterdam waarop hij berichten ontving die blijkbaar zagen op de moord, en dat deze telefoon eerder niet door hem was gebruikt. Deze omstandigheid werd door de rechtbank als bewijs gebruikt voor de voorbedachte raad van de dader, en het feit dat de telefoon uitpeilde op de plaats delict ten tijde van de liquidatie werd ook tot het bewijs gebezigd. Het vonnis werd (tot op heden) niet gepubliceerd.[122]

Mensenhandel Amsterdam.
Op 2 mei 2013 veroordeelt de rechtbank Amsterdam twee mannen tot meerjarige gevangenisstraffen omdat zij met intimidatie en bedreiging twee vrouwen, van wie één slechts achttien jaar oud was, in de prostitutie hebben gebracht. De rechtbank overweegt daarbij dat de verklaringen van de slachtoffers, die worden bestreden door de verdachten, in belangrijke mate worden ondersteund door de historische telefoongegevens van beide verdachten. De vonnissen werden niet gepubliceerd.[123]

Beroving met geweld van pizzakoerier.
Een pizzakoerier wordt aangevallen en beroofd. Hij wordt zo hard geslagen en geschopt dat hij enige tijd buiten westen is en zich niets meer kan herinneren als hij weer bijkomt. Zijn jas zit onder het bloed en zijn trouwring, portemonnee en horloge zijn gestolen, evenals zijn pizza’s. Hij wordt met een hersenschudding in het ziekenhuis opgenomen. Onderzoek naar het IP-adres gebruikt bij de online bestelling waar de koerier heen ging en het daarbij opgegeven telefoonnummer leiden naar een verdachte. Deze ontkent aanvankelijk dat hij de gebruiker was van de betreffende telefoon, maar door middel van historische telecomgegevens uit de periode voorafgaand aan de overval kan dat worden aangetoond, waarna hij dat erkent. Op 30 oktober 2014 veroordeelt de rechtbank Amsterdam hem tot drie jaar gevangenisstraf.[124] Het vonnis is niet gepubliceerd.

Georganiseerde handel in illegaal vuurwerk.
In april 2013 wordt een man veroordeeld voor de georganiseerde handel in illegaal vuurwerk. Hij heeft meer dan duizend kilo zwaar en illegaal vuurwerk zonder veiligheidsmaatregelen opgeslagen in een woning, garagebox en auto, met grote veiligheidsrisico’s voor de omwonenden tot gevolg. De man bood zijn vuurwerk aan via internet en kon alleen worden opgespoord door het opvragen van internetgegevens en

[122] Parketnummer 13/665330-13
[123] Parketnummers o.a. 13/708141-12.
[124] Parketnummers 13/650958-13(A), 13/659298-14(B), niet gepubliceerd.

(prepaid) telefoongegevens gekoppeld aan zijn handel. Het vonnis vermeldt dat niet, en is ook niet gepubliceerd.[125]

Marktplaats overvaller.

Ook kan genoemd worden de veroordeling op 19 september 2014 van een gewelddadige overvaller die zijn slachtoffers uitzocht aan de hand van hun Marktplaats-advertenties. Hij kon worden gevonden door onderzoek te doen naar het IP-adres dat hij gebruikte om de advertenties van zijn slachtoffers op Marktplaats te bekijken en hij bekende nadat hij geconfronteerd werd met het feit dat zijn mobiele telefoon was gelokaliseerd bij verschillende overvallen. Het Gerechtshof Amsterdam veroordeelde hem tot vier jaar gevangenisstraf, maar kon in zijn arrest volstaan met het aanhalen van de aangiftes en de bekentenis van de overvaller, en publiceerde het arrest bovendien niet op rechtspraak.nl.[126]

Hacks en DDOS aanval tegen KPN en anderen.

Op 7 juni 2013 veroordeelt de rechtbank Rotterdam een minderjarige verdachte voor het hacken van KPN, het beheren van een website met gestolen creditcardgegevens, de hack op een universiteit en een (D)DOS-aanval op internet security bedrijf Fox-IT dat onderzoek deed voor KPN betreffende de hack.

De afdeling webcare van KPN werd via Twitter gewaarschuwd voor een hack in de systemen van KPN. Uit het onderzoek door KPN, Fox-IT en later ook de politie aan de systemen van KPN is vervolgens zicht ontstaan op verschillende IP-adressen. Dat was al enige tijd nadat de hack op het systeem plaatsvond. Omdat uit onderzoek naar de IP-adressen bleek dat gebruik gemaakt werd gemaakt van afschermingstechnieken en de gebruikte IP adressen zich over de hele wereld bevonden, nam het geruime tijd in beslag om de juiste IP-adressen vast te stellen en vervolgens de bij deze IP-adressen behorende identificerende gegevens te verkrijgen door middel van rechtshulp, te analyseren en vervolgens door te kunnen rechercheren op andere relevante IP-adressen. Uitsluitend door onderzoek naar historische gegevens van deze IP-adressen (historische NAW-gegevens, historische verkeersgegevens en overige historische gegevens) en door patronen in deze gegevens te ontdekken, in combinatie met (technisch) onderzoek naar de gebruikte nickname, is zicht ontstaan op de hacker. Anders dan zou kunnen worden geconcludeerd bij alleen een eerste blik op de IP-adressen, namelijk het gebruik van locaties over de hele wereld, bleek de hacker zich uiteindelijk gewoon in Nederland te bevinden.

Om de verkregen inzichten vervolgens te kunnen verifiëren was het noodzakelijk om de historische gegevens van deze specifieke verdachte te bevragen, te analyseren en te leggen naast de resultaten uit de overige en eerdere opsporingsmiddelen om patronen te ontdekken. Inmiddels waren reeds enkele maanden na de start van het onderzoek verstreken. Naast het specifieke technische onderzoek hebben derhalve historische gegevens van meerdere maanden oud een cruciale rol gespeeld in het kunnen identificeren van de verdachte. Zonder de mogelijkheid om gedurende langere tijd historische gegevens van IP-adressen te kunnen bevragen zou dit onderzoek door

[125] Rechtbank Noord-Holland 4 april 2013, parketnummer 15/997508-11.
[126] Gerechtshof Amsterdam 19 september 2014, parketnummer 23/001083-14.

tijdsverloop gestrand zijn bij een IP-adres in het buitenland omdat de vervolggegevens dan zouden ontbreken.
Gedurende het onderzoek bleek dat sprake was van meerdere hacks, het beheren van een website met gestolen creditcardgegevens, alsmede dat verdachte de website van het internetsecurity bedrijf dat door KPN betrokken was bij onderzoek naar de hack had platgelegd. Uit het onderzoek is ook gebleken dat de hacker zeer ver in de systemen van KPN was binnengedrongen, zich toegang had verschaft tot servers met klantgegevens van particulieren en bedrijven zoals adressen, telefoonnummers en bankrekeningnummers, en zeer grote schade had kunnen aanrichten. De uitspraak in deze zaak is niet gepubliceerd.[127] Er is wel uitvoerig over bericht in de media.[128]

Dit zijn slechts enkele voorbeelden.
Er zijn vele andere ongepubliceerde vonnissen over zaken waarin historische telecomgegevens belangrijk waren voor de opsporing of voor het bewijs werden gebruikt, waaronder bijvoorbeeld:

- Rechtbank Rotterdam 12 februari 2015, mensenhandel waarbij een minderjarig meisje door meerdere daders in de prostitutie is gebracht[129]
- Rechtbank Noord-Holland 14 augustus 2014, groot aantal woninginbraken[130]
- Rechtbank Amsterdam 19 juni 2014, mensenhandel, uitbuiting van acht vrouwen in de prostitutie[131]
- Rechtbank Amsterdam 18 juni 2014, gewelddadige overval met een vuurwapen op een café[132]
- Rechtbank Amsterdam 10 juli 2012, grootschalige drugshandel[133]
- Rechtbank Utrecht 1 mei 2011, gijzeling met vuurwapens en ernstig geweld in het Utrechtse criminele milieu[134]

De meeste strafrechtelijke uitspraken worden dus niet gepubliceerd, waaronder zeer vele over ernstige strafbare feiten waarvan de daders opgespoord konden worden door gebruik te maken van historische telecomgegevens.

<u>Niet alle vonnissen noemen het gebruik van telecomgegevens, ook als dat voor het onderzoek wel doorslaggevend is geweest.</u>

Rechters moeten efficiënt zijn in het schrijven van hun vonnissen. Zij gaan dus niet altijd op alle bewijsmiddelen in, en doen dat zeker niet in altijd in detail. Vaak worden de voor een veroordeling gebruikte bewijsmiddelen vermeld in een bijlage bij het vonnis, en niet in het vonnis zelf. Die bijlagen worden soms wel, maar meestal niet gepubliceerd op rechtspraak.nl. In de meeste vonnissen wordt ook geen uitgebreide beschrijving gegeven

[127] Parketnummer 10/960020-12.
[128] Zie bijv. http://www.nrc.nl/nieuws/2012/02/08/kpn-slachtoffer-van-computerhack/.
[129] Parketnummers o.a. 10/750229-13.
[130] Parketnummers o.a. 15/810034-14.
[131] Parketnummers o.a. 13/520056-09.
[132] Parketnummers 13/669115-13 en 13/665834-13.
[133] Parketnummers o.a. 13/706316-11.
[134] TGO Jutfaas. Parketnummers o.a. 16/600665-10, 16/711992-10, 16-600577-10, 16-711329-10.

van het verloop van het onderzoek, maar concentreert de rechter zich op de rechtsvragen die beantwoord moeten worden. Het gevolg is dat uit verreweg de meeste op rechtspraak.nl gepubliceerde vonnissen moeilijk of geheel niet valt af te leiden welke opsporingsmiddelen (met succes) gebruikt zijn voor de opsporing en voor het bewijs.

Soms is uit een korte vermelding op te maken dat historische telecomgegevens van belang waren.

Mensenhandel minderjarige slachtoffers.
Exemplarisch zijn bijvoorbeeld twee vonnissen uit november 2014 waarin de rechtbank Noord-Nederland kortweg opmerkt dat de verklaringen van twee minderjarige slachtoffers worden bevestigd door telefoon- en internetgegevens, ook op details.[135] De verdachten in die zaak worden veroordeeld tot langdurige gevangenisstraffen voor het in de prostitutie brengen van twee minderjarige meisjes.

Woningoverval bejaard slachtoffer.
Ook illustratief is een vonnis van 27 november 2014 waarin een dader wordt veroordeeld van een woningoverval waarbij een 76-jarige man de trap op is gesleept, met een mes bedreigd, in het gezicht gestompt en op bed vastgebonden, waarna de daders zijn huis hebben doorzocht en onder meer de trouwring van zijn overleden vrouw van zijn vinger hebben getrokken, om het slachtoffer daarna in hulpeloze toestand achter te laten. In het vonnis zelf worden historische telecomgegevens niet genoemd. Alleen wie doorleest tot de bijlage met bewijsmiddelen constateert dat de rechtbank een zogenaamde netwerkmeting voor het bewijs gebruikt, waaruit blijkt dat de telefoon van de verdachte tijdens de overval een telefoonmast bij de woning van het slachtoffer aanstraalde.[136]

Met grote regelmaat worden telecomgegevens helemaal niet in het vonnis genoemd als bewijsmiddel, maar zijn ze van groot belang geweest voor de opsporing omdat ze het onderzoek richting geven. Bijvoorbeeld omdat ze uitwijzen met wie een verdachte contact heeft gehad, die daarna als getuige een belangrijke verklaring aflegt. Of omdat een verdachte bekent als hij met zijn internet- of belgedrag wordt geconfronteerd. In zulke gevallen hebben telecomgegevens het onderzoek een doorslaggevende duw gegeven, maar worden ze in het vonnis niet genoemd: het aanhalen van de verklaring of bekentenis die het resultaat is, is immers genoeg.

Poging doodslag na seksafspraak via internet.
In een vonnis van 16 december 2014 noemt de rechtbank Limburg het onderzoek naar de telecommunicatie en het gebruikte IP-adres alleen in de weergave van het standpunt van de officier van justitie, maar gaat er verder in het vonnis niet op in. De (bekennende) verdachte wordt veroordeeld voor poging doodslag en oplichting.[137]

---

[135]http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBNNE:2014:5621 en http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBNNE:2014:5620.
[136] Zie E http://deeplink.rechtspraak.nl/uitspraak?id=CLI:NL:RBOVE:2014:6942.
[137] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBLIM:2014:10916.

DDOS-aanvallen op websites, hacking en bedreiging.
Op 14 april 2010 veroordeelt de rechtbank Rotterdam verdachte voor DDOS-aanvallen op websites, bedreiging, hacking en creditcardfraude.[138] Nu verdachte de feiten deels heeft bekend en geen verweren heeft gevoerd over de wijze waarop hij is geïdentificeerd, is in het vonnis geen aandacht voor de identificatie van verdachte. Deze heeft echter in grote mate plaats gevonden door analyse van IP-adressen die bij de DDOS-aanvallen werden gebruikt.

Kinderporno van eigen dochter en haar vriendinnen.
Een ander veelzeggend voorbeeld is de veroordeling in juni 2014 van een man die kinderpornografische foto's maakte van zijn dochter en verschillende van haar vriendinnetjes, en die op het internet plaatste.[139] Nergens in het vonnis komen telecomgegevens ter sprake. De rechtbank concentreert zich op een bespreking van het in de woning van de man in beslag genomen materiaal en zijn (gedeeltelijk bekennende) verklaringen daarover. De doorzoeking en aanhouding van deze man konden plaatsvinden doordat de historische gegevens konden worden opgevraagd van het IP-adres waarmee hij zijn zelfgemaakte kinderporno op een website had geplaatst.

Beïnvloeding getuige.
In november 2013 veroordeelt de rechtbank Amsterdam verschillende daders, waaronder een advocaat, voor het beïnvloeden van een getuige. Deze getuige is - kort voordat hij een verklaring moest afleggen bij de rechter-commissaris over een miljoenenfraude - opgehaald door verschillende verdachten, 's nachts naar het kantoor van de advocaat gebracht en daar uitgebreid geïnstrueerd wat hij wel en niet moest verklaren bij de rechter-commissaris. Als de getuige dat vertelt, ontkennen alle verdachten dat eerst geheel. Dat verandert als de verdachten worden geconfronteerd met het onderzoek naar de historische telefoongegevens, waaruit een belangrijk overzicht van onderlinge contacten en reisbewegingen kan worden verkregen dat het relaas van de getuige bevestigt. Daarop passen de verdachten hun verklaringen aan en bekennen gedeeltelijk. De officier van justitie ging in zijn requisitoir uitgebreid in op het belang van de historische telecomgegevens, maar de rechtbank constateert slechts dat de verklaringen van de getuige "na verificatie juist zijn gebleken". Van de verschillende vonnissen in deze zaak worden er twee op rechtspraak.nl gepubliceerd, en drie andere niet.[140]

Stalking ex-vriendin.
Op 12 november 2014 wordt een man veroordeeld voor o.a. belaging en bedreiging van zijn ex-vriendin.[141] Dit deed hij (vooral) via internet, een soort cyberstalking. Zijn ex-vriendin runde een pension. Verdachte heeft vervolgens gedurende een langere periode

---

[138] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBROT:2010:BM1172
[139] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBMNE:2014:2657.
[140] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2013:7270 en http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2013:7269. Zie ook https://www.om.nl/actueel/nieuwsberichten/@32282/celstraffen-negen/.
[141] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBOBR:2014:6814

valse negatieve beoordelingen geplaatst op een groot aantal beoordelingssites Hij ging daarbij geraffineerd te werk. Hij plaatste aanvankelijk beoordelingen vanaf zijn eigen pc/internetaansluiting, maar toen die na een paar beoordelingen geweigerd werden (maximum aantal beoordelingen vanaf één IP voor een accommodatie) ging hij met zijn laptop de omgeving af voor open netwerken van anderen en gebruikte hij internetverbindingen van familieleden. Al hoewel dit uit het vonnis van de rechtbank niet blijkt, hebben historische gegevens van IP-adressen een grote rol gespeeld om verdachte op het spoor te komen, mede gelet op zijn ontkennende houding. Om het digitale spoor te kunnen volgen waren de historische NAW-gegevens van de IP-adressen en emailadressen van de berichten op de beoordelingssites noodzakelijk.

Bedreiging diverse politici via Twitter.
Op 19 april 2011 veroordeelt[142] de rechtbank Rotterdam een man voor het via Twitter bedreigen van landelijke politici van GroenLinks, de PvdA en D66. De man had onder meer op twitter.com de volgende tekst geplaatst: *"@(aangever)? Zal je toekijken als ik je kleine dochtertje helemaal uit elkaar trekt?"* en *"Wie zal ik morgen als eerste zijn nek doorsnijden? #(aangever 3) of #(aangever 4)?"*
De rechtbank constateert in haar vonnis dat het bedreigen van politici een bedreiging kan betekenen voor het functioneren van de parlementaire democratie en in dit geval tot gevolg heeft gehad dat de kinderen van een van de betrokken politici enige dagen permanent zijn beveiligd en zoveel mogelijk binnen moesten blijven. Verdachte kon opgespoord worden op basis van de historische gegevens van het IP-adres van de (anonieme) plaatser van de tweets. Uit het vonnis blijkt dat niet.

De webcamhacker.
Op 4 september 2014 veroordeelt de rechtbank Rotterdam een verdachte voor het op grote schaal inbreken op computers van anderen en het overnemen van gegevens van die computers. [143] Verdachte heeft maandenlang stelselmatig webcams van zijn slachtoffers aangezet door verspreiding van malware. Hierdoor kon hij ongemerkt zijn slachtoffers, veelal jonge meisjes, begluren. Op deze wijze heeft verdachte honderden mensen bespied en een enorme hoeveelheid computerdata binnengehaald (ruim 41 miljoen afbeeldingen). Hij categoriseerde maandenlang de binnengehaalde beelden, waaronder veel beelden van jonge meisjes die naakt waren en met zichzelf of anderen seksuele handelingen verrichtten. Verder bezat de verdachte ook harde kinderporno die hij van gehackte computers had gedownload en heeft hij de computer van een ander gebruikt om de examenfraudezaak uit 2013 aan het licht te brengen, waardoor die persoon ten onrechte als verdachte werd aangemerkt.
Dit onderzoek is gestart en opgelost door sporen van IP-adressen te volgen, beginnend met de aangifte van een minderjarig meisje dat aangifte doet omdat zij ziet dat een eigen naaktfilmpje door iemand anders op haar eigen Facebook-account is geplaatst, daarmee zichtbaar voor 300 contacten. Onderzoek aan haar computer levert op dat haar computer

[142] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBROT:2011:BQ1814
[143] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBROT:2014:7379 en http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBROT:2014:7380 (omdat de verdachte een deel van de feiten pleegde toen hij minderjarig was en een deel toen hij meerderjarig was zijn er twee vonnissen die zien op dezelfde verdachte).

is gehackt. De malware op haar computer heeft dat filmpje gezonden naar een bepaald IP-adres; de hacker heeft het vervolgens op haar gehackte Facebook-account geplaatst. Het onderzoek start op het IP-adres waarnaar de malware het filmpje heeft gestuurd. Hetzelfde IP-adres blijkt voor te komen in twee andere onderzoeken en leidt naar het woonadres van verdachte. Uiteindelijk blijken minimaal 2.000 computers door verdachte gehackt/begluurd te zijn, bij sommige slachtoffers meer dan een jaar lang. Dankzij het onderzoek konden de slachtoffers worden geïnformeerd en konden maatregelen getroffen worden om de besmette computers te schonen. Omdat de verdachte bekende heeft de rechtbank in het vonnis geen aandacht besteed aan de wijze waarop hij is opgespoord. Het is echter zonneklaar dat zonder historische gegevens van het gebruikte IP-adres dit alles niet aan het licht zou zijn gekomen.

Historische telecomgegevens worden ook gebruikt voor rechtshulp en de opsporing van voortvluchtigen.

Historische telecomgegevens worden niet alleen opgevraagd om in Nederlandse onderzoeken de feiten op te helderen over gepleegde misdrijven, maar ook:

- op verzoek van andere landen voor buitenlandse strafrechtelijke onderzoeken (rechtshulp)
- om voortvluchtige verdachten en ontsnapte gevangenen en TBS-ers op te sporen

De resultaten van deze bevragingen zijn vrijwel nooit in de Nederlandse jurisprudentie terug te lezen. Immers, buitenlandse strafrechtelijke onderzoeken leiden tot vonnissen in het buitenland, niet in Nederland. De wijze waarop voortvluchtige verdachten aangehouden konden worden, wordt doorgaans niet besproken in Nederlandse vonnissen omdat de rechter daar geen oordeel over hoeft te vellen. Als ontsnapte gevangenen en TBS-ers worden opgespoord aan de hand van historische telecomgegevens leidt dat niet tot nieuwe vonnissen.

Wat een gebrek aan historische telecomgegevens kan betekenen voor de opsporing van voortvluchtigen blijkt uit het al genoemde rapport van de Europese Commissie. Daarin wordt beschreven hoe een Poolse moordverdachte die vermoedelijk in Duitsland verbleef niet kon worden opgespoord omdat de door de voortvluchtige gebruikte IP-adressen in Duitsland niet bewaard waren.[144]

Wanneer is het opvragen van telecomgegevens succesvol?

Het kwantificeren van het gebruik van historische telecomgegevens kan dus niet gebeuren aan de hand van gepubliceerde jurisprudentie. Daarvoor wordt er te weinig jurisprudentie gepubliceerd, en geven vonnissen te vaak geen inzicht in de rol die telecomgegevens hebben gespeeld in de opsporing. Bovendien geven vonnissen geen zicht op het belang van historische telecomgegevens voor rechtshulp en de opsporing van voortvluchtigen.

---

[144] Zie http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf, p. 12 nr. 7.

Het is ook niet goed mogelijk om op andere wijze inzicht te geven in de vraag hoe vaak precies het opvragen van historische telecomgegevens bijdraagt aan de opsporing van strafbare feiten. Dat komt door verschillende complicerende factoren.

In de eerste plaats rijst bij de vraag naar het doorslaggevend belang of het ‘succespercentage’ de vraag wiens oordeel doorslaggevend is: dat van de politie, het Openbaar Ministerie of de rechter? Een voorbeeld kan dat illustreren:

Gewelddadige woningovervallen.
Op 8 juli 2014 wordt een verdachte door de rechtbank Rotterdam veroordeeld tot vier en een half jaar gevangenisstraf voor een gewelddadige woningoverval waarbij een moeder en drie jonge kinderen met een pistool zijn bedreigd en zijn vastgebonden. De dader wordt vrijgesproken van een andere gewelddadige woningoverval. Verdachte kwam pas lange tijd na deze woningovervallen in beeld van de politie door een tip uit het publiek. Op dat moment was de eerste woningoverval meer dan een jaar geleden, zodat geen historische telefoongegevens meer gevorderd konden worden voor de dag van die overval. De tweede overval was minder dan een jaar geleden, en uit de historische telefoongegevens bleek dat de telefoon van de verdachte tijdens de overval uitpeilde bij de plaats delict. Bij beide woningovervallen is DNA van de verdachte aangetroffen: bij de eerste overval op achtergelaten duct tape en bij de tweede overval op een achtergelaten horlogebandje. Nergens in het vonnis noemt de rechtbank de historische telefoongegevens, terwijl de officier van justitie deze gegevens van belang vond voor het bewijs voor de tweede overval en daarop in haar requisitoir uitgebreid is ingegaan.[145]
Is het opvragen van de telefoongegevens in deze zaak nu onsuccesvol geweest omdat ze in het vonnis niet worden genoemd? Het is bepaald denkbaar – gelet op het verschil tussen vrijspraak voor de overval zonder telefoongegevens en veroordeling voor de overval met telefoongegevens - dat de telefoongegevens hebben bijgedragen aan de overtuiging van de rechters voor de tweede overval, maar weten doen we dat niet. En als in hoger beroep het Hof de telefoongegevens wel voor het bewijs gebruikt, moet de conclusie dan worden aangepast en wordt het opvragen van de telefoongegevens in deze zaak dan alsnog succesvol? En als het in een andere zaak andersom is: de rechter in eerste aanleg gebruikt de telefoongegevens wel voor het bewijs en in hoger beroep wordt de dader ook veroordeeld maar de telefoongegevens niet genoemd, is het opvragen van de telefoongegevens dan succesvol geweest of niet?

Het gebeurt regelmatig dat de officier van justitie, de rechter in eerste aanleg en de rechter in tweede aanleg niet hetzelfde denken over de bewijswaarde van historische telecomgegevens. Een ander voorbeeld - dat nog onder de rechter is - betreft een onderzoek tegen een man die wordt verdacht van twee verkrachtingen in Hoorn in 2011. De rechtbank Alkmaar veroordeelde de man in 2012 voor één verkrachting, maar sprak hem vrij van de andere.[146] De in het onderzoek opgevraagde historische telefoongegevens van de man worden nergens in het vonnis genoemd. Het Openbaar Ministerie heeft zowel bij de rechtbank als bij het hof de telefoongegevens van de verdachte als belastend bewijs aangevoerd. Het hof moet nog over de zaak oordelen.

[145] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBROT:2014:5550.
[146] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBALK:2012:BX4587.

Ook een vonnis van de rechtbank Midden-Nederland van 31 januari 2014 roept de vraag op wanneer het opvragen van historische telecomgegevens succesvol is. De zaak betreft twee verdachten die ’s ochtends vroeg in een auto worden aangetroffen met de buit van een inbraak die nacht. De historische telefoongegevens van de verdachten worden gevorderd, en daaruit blijkt dat de verdachten onderling telefonisch contact hebben gehad en dat hun telefoons telefoonmasten hebben aangestraald die zijn gelegen op de route tussen de woning waarin is ingebroken en de woning van een van de verdachten. Desalniettemin spreekt de rechtbank in het enige gepubliceerde vonnis in deze zaak de verdachte vrij omdat ‘onduidelijk is wanneer verdachte is ingestapt en welke wetenschap hij had van de aanwezige goederen’ en omdat ‘niet vaststaat dat de telefoon tijdens het afleggen van de route daadwerkelijk in handen was van de verdachte’.[147] Ook hier de vraag: is dit een voorbeeld van succesvol gebruik van historische telecomgegevens in de opsporing of niet? En wordt dat anders als de daders in een hoger beroep wel veroordeeld worden (hetgeen niet ondenkbaar is, gelet op het feit dat in vele soortgelijke gevallen verdachten wel veroordeeld zijn)?

Zie verder bijvoorbeeld:

- Rechtbank Overijssel 5 maart 2015, officier concludeert tot veroordelingen voor poging tot afpersing mede op grond van historische telefoongegevens maar rechtbank spreekt vrij[148]
- Rechtbank Noord-Holland 26 februari 2015, zaak Michelle Mooij: officier concludeert tot veroordeling, rechtbank gebruikt historische telefoongegevens wel voor reconstructie en veroordeelt voor verkrachting en mishandeling maar spreekt vrij van moord/doodslag[149]
- Rechtbank Gelderland 26 juni 2014, officier concludeert tot veroordelingen voor diefstal met geweld mede op grond van historische telefoongegevens maar rechtbank spreekt vrij[150]

Zo zijn er vele zaken die illustreren dat men op basis van het dossier verschillend kan denken over de (bewijs)waarde van telecomgegevens.

In de tweede plaats rijst de vraag wanneer het opvragen van telecomgegevens succesvol is. Alleen als ze voor het bewijs worden gebruikt? Of ook als ze leiden tot een bekentenis of een voor het bewijs belangrijke getuigenverklaring? Als ze er toe leiden dat de verdachte een eerdere leugenachtige verklaring intrekt maar niet bekent? Als ze er juist toe leiden dat de onjuistheid van een getuigenverklaring kan worden vastgesteld, zodat die in het proces verder buiten beschouwing kan worden gelaten? Als aan de hand van historische telecomgegevens een alternatief scenario kan worden uitgesloten? Is het

[147] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBMNE:2014:1150.
[148] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBOVE:2015:1127 en http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBOVE:2015:1124 en http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBOVE:2015:1125 en http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBOVE:2015:1126.
[149] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBNHO:2015:1471.
[150] Zie o.a. http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBGEL:2014:3918.

opvragen succesvol als aan de hand van historische telefoongegevens de reisbewegingen van een verdachte kunnen worden vastgesteld, waardoor een tot dan toe onbekende verblijfplaats wordt ontdekt waarin relevant bewijsmateriaal wordt gevonden? Of als er aan de hand van historische telefoongegevens een telefoonnummer van een medeverdachte wordt gevonden dat vervolgens getapt kan worden waardoor belastende gesprekken kunnen worden opgenomen? Is dat dan alleen een 'succes' van het aftappen, of ook van het gebruik van historische telefoongegevens dat het aftappen mogelijk maakte?

Doorgaans is uit een vonnis niet op te maken wat het belang is geweest in een onderzoek van historische telecomgegevens. Wat moeten we bijvoorbeeld concluderen over het vonnis van de rechtbank Amsterdam van 5 december 2013[151] waarin een verdachte wordt veroordeeld tot acht jaar gevangenisstraf voor doodslag bij een woningoverval? Omdat de verdachte bekent hoeven er geen telecomgegevens voor het bewijs gebruikt te worden. Bij de verwerping van een alternatief scenario van de verdediging verwijst de rechtbank wel naar historische telefoongegevens en een tijdslijn die de politie heeft opgesteld van de gebeurtenissen. Welk vakje moet in zo'n geval worden aangekruist: 'succesvol', of 'niet succesvol'?

Dezelfde vraag geldt voor de zaak van een serie-aanrander die op 22 januari 2015 door de rechtbank Noord-Holland wordt veroordeeld voor vier aanrandingen in Den Haag, en van vier andere aanrandingen wordt vrijgesproken.[152] In het onderzoek is een tijdslijn gereconstrueerd van alle delicten en de mogelijke betrokkenheid van de verdachte daarbij, waarbij historische telecomgegevens een belangrijke rol speelden. De verdachte heeft uiteindelijk, pas nadat hij is geconfronteerd met zijn telecomgegevens, vier aanrandingen (min of meer) bekend en vier andere ontkend. De rechtbank veroordeelt hem alleen voor de aanrandingen die hij (min of meer) bekent, en spreekt hem van de andere vrij. In het hele vonnis wordt het telecomonderzoek nergens genoemd.[153] Of het telecomonderzoek er toe heeft bijgedragen dat de verdachte deels heeft bekend weten we niet: we kunnen niet in zijn hoofd kijken. Is hier nu succesvol gebruikt gemaakt van historische telecomgegevens omdat deze gegevens voor politie en Openbaar Ministerie belangrijk waren bij het reconstrueren van de misdrijven en de verdachte deels bekende nadat hij met deze gegevens geconfronteerd werd, of niet omdat de rechter ze niet voor het bewijs heeft gebruikt?

In strafrechtelijke onderzoeken worden steeds verschillende opsporingsmethoden gebruikt in onderlinge samenhang. Zowel klassieke opsporingsmethoden (observatie, verhoren van getuigen, aangevers en/of verdachten, het doorzoeken van woningen of auto's, het onderzoeken van sporen op de plaats delict, telefoontaps, het vorderen van andere historische gegevens dan telecommunicatiegegevens, etc.) als opsporing door gebruikmaking van historische telecomgegevens leveren een wezenlijke bijdrage aan het eindresultaat. Het is doorgaans niet goed mogelijk de gebruikte opsporingsmethoden in een onderzoek los van elkaar te zien. Voor het bereiken van een resultaat, waaronder ook

[151] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2013:8400.
[152] Zie
[153] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBNHO:2015:675.

het uitsluiten van betrokkenheid van personen (bijvoorbeeld door het controleren van een alibi), is het nodig alle mogelijke opsporingsmethoden in onderlinge samenhang te gebruiken. Resultaat wordt doorgaans geboekt door opsporingsmethoden te combineren, waarbij het niet mogelijk is om achteraf succes aan één specifieke methode toe te schrijven. Om een beeldspraak te gebruiken: als een aannemer wordt gevraagd voor ieder stuk gereedschap precies aan te geven hoeveel het heeft bijgedragen aan de bouw van verschillende opgeleverde huizen, zal hij zeer waarschijnlijk ook het antwoord schuldig moeten blijven.

In de derde plaats geldt dat historische telecomgegevens ook van groot belang kunnen zijn voor de opsporing als het opsporingsonderzoek uiteindelijk niet leidt tot een strafzaak. Eerder in dit rapport noemden we al verschillende zaken waarin het onderzoek van telecomgegevens belangrijk ontlastend bewijs opleverde. Een ander voorbeeld kan dit punt nader illustreren:

Bommelding IKEA Amsterdam 2009.
Op 11 maart 2009 kwam bij de meldkamer van de politie Amsterdam een anonieme melding binnen over een op handen zijnde aanslag de volgende dag bij de IKEA en de Mediamarkt in Amsterdam. Daarbij werden namen en verblijfplaatsen genoemd van personen die die aanslag zouden gaan plegen. Gelet op de inhoud van de melding werd onmiddellijk ingegrepen: de genoemde verblijfplaatsen werden doorzocht, de daar aanwezige personen werden aangehouden en het in de melding genoemde gebied werd ontruimd.[154] Omdat de in de melding genoemde personen op deze adressen niet werden aangetroffen, kon nog niet worden uitgesloten dat zij elders in Nederland verbleven en (alsnog) een aanslag voorbereidden.
De melding was gedaan met een prepaid-telefoon vanuit België. Door onderzoek naar de historische gegevens van die telefoon over een langere periode voorafgaand aan de melding kon worden vastgesteld bij wie deze telefoon in gebruik was. Daarmee kon de kring van personen worden vastgesteld waaruit de melding afkomstig was. Omdat ten tijde van de melding meerdere personen aanwezig waren in het pand van waaruit de melding waarschijnlijk was gedaan en stemherkenning niet uitwees wie de melder was, viel echter niet te bewijzen wie de melder was geweest. Door dit onderzoek, waarin de historische telefoongegevens over een langere periode doorslaggevend waren, kon echter wel worden vastgesteld dat de melding vals was en er geen gevaar voor een aanslag meer dreigde.

Was het opvragen van telefoongegevens in dit geval onsuccesvol omdat er uiteindelijk niemand is veroordeeld, of succesvol omdat daarmee kon worden vastgesteld dat er geen gevaar voor een aanslag meer dreigde?

Het is, om al deze redenen, voor politie en OM niet mogelijk om in cijfers aan te geven in hoeveel zaken het opvragen van historische telecomgegevens 'succesvol' is geweest voor de opsporing. Om dezelfde reden kan overigens van geen enkel opsporingsmiddel met

[154] Zie bijv. http://www.ad.nl/ad/nl/1012/Nederland/article/detail/1998655/2009/03/12/Bommelding-had-terroristische-achtergrond.dhtml.

statistieken de noodzaak worden onderbouwd: ook niet van telefoontaps, doorzoekingen, getuigenverhoren, observaties, etc.
Wel kunnen we zonder voorbehoud concluderen dat het kunnen opvragen van historische telecomgegevens, ook over een langere periode, van essentieel belang is voor de opsporing van zeer vele verschillende ernstige strafbare feiten. Het verdient dus nadruk dat de meer dan honderd recente vonnissen die in dit rapport worden genoemd slechts voorbeelden zijn, het topje van de ijsberg: er zijn heel veel andere zaken waarin historische telecomgegevens belangrijk waren voor de opsporing en het bewijs.

Hoofdstuk 4. Worden de voor de opsporing benodigde gegevens niet bewaard als er geen bewaarplicht is?

In het publieke debat over de bewaarplicht wordt soms, zonder onderbouwing, gesteld dat voor de opsporing benodigde telecomgegevens ook wel bewaard worden door telecombedrijven voor hun bedrijfsvoering, zodat het niet noodzakelijk is tot bewaring te verplichten.[155]

Er zijn duidelijke aanwijzingen dat het tegendeel het geval is. Verschillende aanbieders van telecommunicatiediensten hebben in een kort geding om volledige afschaffing van de bewaarplicht gevraagd en daartoe aangevoerd dat zij thans gegevens bewaren die zij zonder bewaarplicht niet zouden bewaren. Deze aanbieders stellen dat zij voor hun eigen bedrijfsvoering telecomgegevens veel korter zouden bewaren, of zelfs de klant de keuze zouden willen geven of en welke gegevens bewaard worden.[156] (Het is niet moeilijk voor te stellen welke keuze criminelen graag zouden maken).[157] Nadat de civiele rechter de bewaarplicht buiten werking heeft gesteld, hebben ook andere aanbieders aangegeven minder gegevens te gaan bewaren en dat korter te gaan doen.

Zonder bewaarplicht is de overheid geheel afhankelijk van de gegevens die providers bewaren voor bedrijfsdoeleinden. Bij zogenaamde flat-fee contracten, waarbij de gebruiker een vast bedrag betaalt onafhankelijk van zijn telefoon- of internetgebruik, is er niet of nauwelijks nog een bedrijfsbelang om verkeersgegevens gedurende langere tijd op te slaan. In Duitsland, waar de bewaarplicht ongrondwettelijk is verklaard, worden IP-adressen niet langer dan een week bewaard, en door sommige providers slechts enkele dagen of zelfs helemaal niet.[158] Om die periode in perspectief te plaatsen: van de vele honderden meldingen die de Nederlandse politie in 2014 kreeg over het uploaden of downloaden van kinderporno door gebruikers van Nederlandse IP-adressen zag meer dan 80% op een pleegdatum ouder dan twee weken. Zonder de mogelijkheid om identificerende gegevens over die IP-adressen op te vragen kan de overgrote meerderheid van dat soort meldingen niet meer onderzocht worden bij gebrek aan andere aanknopingspunten voor onderzoek.

Het voorbeeld van de online kindermisbruiker die op 12 februari 2015 is veroordeeld door de rechtbank Amsterdam, hierboven beschreven, spreekt ook voor zich: als IP-adressen maximaal een week bewaard worden, zoals in Duitsland, is er niet of nauwelijks onderzoek mogelijk naar bedreiging en misbruik via internet waarvan meer dan een week na het feit aangifte wordt gedaan, bijvoorbeeld omdat het enige tijd duurt voordat ouders ontdekken dat hun kind (online) slachtoffer is geworden.

---

[155] Zie bijvoorbeeld kamerstukken 33 939, nr. 3, p. 3.
[156] Zie http://www.boekx.com/uploads/publicaties/Dagvaarding_kg_Wet_Bewaarplicht_Telecommunicatie.pdf, p. 9-10.
[157] Zie bijv. http://tweakers.net/nieuws/101850/vodafone-kpn-telfort-en-xs4all-stoppen-met-uitvoeren-bewaarplicht.html.
[158] Zie http://www.netzwelt.de/news/91086-ip-speicherfristen-lange-speichern-anbieter.html.

Dat zonder bewaarplicht de voor de opsporing benodigde gegevens om andere redenen wel beschikbaar blijven bij providers, wordt ook weersproken door een rapport van de Europese Unie over dataretentie in de Europese Unie.[159] Daarin worden tal van voorbeelden uit vele Europese landen gegeven van het gebruik van telecomgegevens voor de opsporing, maar ook voorbeelden van de gevolgen van het ontbreken van de gevraagde gegevens. Die laatste voorbeelden komen met name uit Duitsland en Tsjechië, waar de constitutionele hoven in respectievelijk 2010 en 2011 de bewaarplicht ongrondwettig verklaarden. Het rapport geeft zowel concrete voorbeelden van onderzoeken die niet konden worden opgelost, bijvoorbeeld omdat een provider al na zeven dagen niet meer de identificerende informatie bij een IP-adres kon leveren, als cijfers over het aantal zaken dat hierdoor onoplosbaar werd.[160] Een overzicht van de Duitse politie geeft eveneens een concreet overzicht van vele zaken die door het ontbreken van telecomgegevens niet konden worden opgelost (deels overlappend met de zaken genoemd in het rapport van de Europese Commissie.[161] Uit beide documenten blijkt dat in Duitsland en Tsjechië na het afschaffen van de bewaarplicht ernstige misdrijven niet konden worden opgelost doordat telecomgegevens al na korte tijd – soms al na enkele dagen of een week – niet meer beschikbaar waren, waaronder moorden, terroristische misdrijven, overvallen, fraude, woninginbraken, smokkel, bommeldingen, ernstige bedreigingen, cybercrime met een botnet en kinderporno.
Daarbij dient dan nog bedacht te worden dat Duitsland en vele andere Europese landen een registratieverplichting hebben voor gebruikers van prepaidtelefoons, waarbij zulke gebruikers bij aankoop van een prepaid SIM-kaart tal van persoonlijke gegevens moeten opgeven. Het Duitse Bundesverfassungsgericht heeft een beroep tegen die registratieplicht voor prepaid SIM-kaarten en een appel op het recht om anoniem te kunnen communiceren in 2012 afgewezen.[162] Dat betekent dat in Duitsland uit die verplichte registratie nog aanknopingspunten voor opsporing gehaald kunnen worden bij gebruik van een prepaidtelefoon. In Nederland is er geen registratieplicht bij de aankoop van een prepaid SIM-kaart, en bestaat zonder bewaarde verkeersgegevens geen aanknopingspunt meer voor de opsporing bij misbruik van een prepaidtelefoon, bijvoorbeeld voor anonieme bommeldingen en bedreigingen.

Op grond van de ervaringen in verschillende andere Europese landen en uitlatingen van telecom aanbieders zelf valt dus te verwachten dat zonder bewaarplicht voor de waarheidsvinding belangrijke telecomgegevens aanzienlijk minder vaak beschikbaar zullen zijn ten behoeve van de opsporing en vervolging. De kortgedingrechter concludeert in het vonnis van 11 maart 2015 dan ook dat de bewaarplicht noodzakelijk en effectief is, dat het buiten werking stellen van de bewaarplicht ‘ingrijpende gevolgen kan

---

[159] Evidence for necessity of data retention in the EU (maart 2013), te raadplegen op http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf.
[160] Zie met name p. 6, 9, 10, 18, en 23-27.
[161] Zie http://www.bka.de/nn_234056/SharedDocs/Downloads/DE/ThemenABisZ/Mindestspeicherfristen/101008PresseinformationMindestspeicherfristen,templateId=raw,property=publicationFile.pdf/101008PresseinformationMindestspeicherfristen.pdf.
[162] Zie http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2012/01/rs20120124_1bvr129905en.html.

hebben voor de opsporing en vervolging van strafbare feiten' en dat die gevolgen 'onomkeerbaar' zijn.[163] Ook de Raad voor de Rechtspraak - die de rechterlijke macht vertegenwoordigt - onderschrijft het belang van de bewaarplicht voor de opsporing en vervolging van strafbare feiten.[164]

---

[163] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2015:2498, r.o. 3.6 en 3.12.
[164] Zie http://www.rechtspraak.nl/Actualiteiten/Nieuws/Pages/Wet-bewaarplicht-telecommunicatiegegevens-buiten-werking-gesteld.aspx.

Hoofdstuk 5. Waarom is het nodig om telecomgegevens langdurig op te slaan? Kan dat niet veel korter?

Het is vaak nodig om oudere telecomgegevens op te vragen voor de opsporing. In 2014 betrof 39% van de bevraagde verkeersgegevens van telefoons gegevens ouder dan 6 maanden. Er zijn verschillende redenen waarom regelmatig telecomgegevens van langere tijd geleden worden gevorderd voor de opsporing.

Het gebeurt vaak dat verdachten pas maanden na een misdrijf in beeld komen bij de politie, bijvoorbeeld door tips van burgers, omdat slachtoffers pas enige tijd na een misdrijf aangifte doen of omdat de daders nog een keer de fout in gaan en daarbij aanwijzingen gevonden worden dat zij eerder ook andere misdrijven hebben gepleegd. De aanhouding na een DNA match in januari 2015 van een verdachte van het doden van voormalig minister mw. Borst in februari 2014 is een duidelijk voorbeeld. Een ander voorbeeld is de hierboven beschreven zaak van online kindermisbruik: omdat de minderjarige slachtoffers uit schaamte niets durven zeggen wordt de zaak pas lang na de gepleegde misdrijven bekend gemaakt bij de politie door de moeder van een van de slachtoffers.

Ook komt het veel voor dat verdachten al wel eerder in beeld zijn, maar nog niet bekend is welke telefoon zij gebruiken. Als dan bijvoorbeeld bij een doorzoeking van hun woning in het onderzoek nog niet bekende (prepaid-)telefoons worden gevonden, is het van belang vast te stellen hoe die zijn gebruikt – ook als dat langere tijd na het misdrijf is.

Bij levensdelicten kan verplaatsing van het lichaam er toe leiden dat pas na langere tijd van onderzoek kan worden vastgesteld op welke plek het slachtoffer om het leven is gekomen en wie daarbij als mogelijke betrokkenen in beeld komen.

Voor internet gerelateerde misdrijven, bijvoorbeeld kinderporno, cybercrime of het aanbieden van drugs of wapens via zogenaamde underground markets, geldt dat zij vaak pas enige tijd na plaatsvinden worden geconstateerd. In de hierboven genoemde zaak van online kindermisbruik, bijvoorbeeld, kwam de eerste aangifte meer dan een maand na de laatste feiten omdat de betrokken kinderen zelf niets durfde te vertellen en de moeder van het eerste slachtoffer pas geruime tijd later ontdekte wat er was gebeurd.

Slachtoffers van mensenhandel, andere zedendelicten, bedreiging, afpersing en andere ernstige misdrijven doen met grote regelmaat pas geruime tijd na het misdrijf aangifte. De redenen daarvoor zijn verschillend, maar omvatten angst voor de daders, financiële afhankelijkheid van uitbuiters, zich niet vrij kunnen bewegen, psychische traumaverwerking of omdat slachtoffers alweer in een nieuwe uitbuitingssituatie betrokken zijn geraakt. Ook voor de gevallen dat iemand pas na maanden besluit om naar de politie te gaan en aangifte te doen, is het noodzakelijk dat historische telecomgegevens nog opgevraagd kunnen worden voor de opsporing.

Als in de opsporing rechtshulp nodig is, leidt dat ook tot vertraging omdat rechtshulpverzoeken pas gedaan kunnen worden na enig eigen onderzoek en bovendien

moeten de verzoeken worden opgesteld, vertaald en beoordeeld. Zo doet en krijgt Nederland met grote regelmaat verzoeken aan en van het buitenland tot het opvragen van historische telecomgegevens die door de benodigde formaliteiten pas weken of maanden later kunnen worden uitgevoerd. Ten opzichte van de periode waarin het misdrijf gepleegd is, zijn dan vaak al maanden verstreken.

Tenslotte geldt dat het opvragen van telecomgegevens van langere tijd geleden ook nodig kan zijn naar aanleiding van verklaringen van verdachten of getuigen die pas langere tijd na het misdrijf worden afgelegd. Een duidelijk voorbeeld is de liquidatie in Antwerpen waarvoor Benaouf A. is veroordeeld. Pas zeven maanden na zijn aanhouding legt hij een verklaring af waarin hij uitgebreid een scenario schetst dat hij onschuldig is, en een inmiddels overleden andere persoon aanwijst als dader. Doordat lang na het misdrijf nog telefoongegevens konden worden opgevraagd, kon worden vastgesteld dat die verklaring onjuist was.

Met de bewaartermijnen zoals deze golden tot 11 maart 2015 konden telecomgegevens die voor de opsporing belangrijk waren al regelmatig niet worden opgevraagd omdat zij te oud waren en buiten de bewaartermijn vielen. Dat geldt met name voor internetgegevens, bijvoorbeeld in de opsporing van kindermisbruik en kinderporno. Met regelmaat worden door de autoriteiten van verschillende landen (besloten) internetfora aangetroffen waar kinderporno wordt uitgewisseld. Bij onderzoek daarnaar kan dan worden vastgesteld van welke IP-adressen kinderporno wordt geüpload en gedownload. Dat onderzoek duurt doorgaans echter enige tijd, bijvoorbeeld omdat op in beslag genomen computers en gegevensdragers digitale bestanden van grote omvang moeten worden geanalyseerd. Als dan wordt vastgesteld dat het uploaden of downloaden al enige tijd voor de inbeslagname heeft plaatsgevonden, is veelal de kritische grens van zes maanden al overschreden om de bij het IP adres behorende gegevens op te vragen die kunnen leiden naar de daders. Ook komt het regelmatig voor dat het bestaan van vrij toegankelijke kinderporno op het internet pas langere tijd na het uploaden wordt geconstateerd.

In Nederland was de bewaartermijn voor internetgegevens zes maanden. Het komt regelmatig voor dat Nederland informatie krijgt over Nederlandse IP adressen die betrokken waren bij het uploaden of downloaden van kinderporno, maar daar geen onderzoek naar kan doen omdat het uploaden of downloaden langer dan zes maanden geleden plaatsvond. Omdat het gebruikte IP-adres in verreweg de meeste gevallen het enige aanknopingspunt vormt, blijven zulke meldingen meestal zonder onderzoek of gevolg.

Een concreet voorbeeld hiervan vormt de internationale bestrijdingsactie genaamd ‘operatie Gondola’. Samenwerking tussen de Italiaanse en Amerikaanse autoriteiten leidde tot identificatie van een groot aantal IP-adressen van bezoekers van een website met kinderporno van de ernstiger soort (waaronder het vastbinden en penetreren van kinderen onder de tien jaar). Die informatie werd gedeeld met vele verschillende landen. Dat leidde in 2011 wereldwijd tot tenminste 207 doorzoekingen en 32 aanhoudingen.[165]

[165] Zie https://www.ice.gov/news/releases/top-story-ice-hsi-targets-child-predators-operation-gondola.

In Amerika werd bij een van deze aanhoudingen ontdekt dat de gebruiker van het IP-adres een basisschoolleraar was die ook in zijn omgeving vele leerlingen had gefilmd.[166]
In Nederland gebeurde er echter niets: in maart 2011 ontving Nederland 104 Nederlandse IP-adressen die de website hadden bezocht in maart 2010 om kinderporno te uploaden of te downloaden. Omdat dat langer dan zes maanden geleden was, konden er geen historische internetgegevens worden verkregen en kon dus geen onderzoek worden verricht naar de gebruikers van deze IP-adressen.[167]

Dezelfde situatie deed zich voor bij de internationale bestrijdingsactie genaamd 'operatie Hydra'.[168] Ook hierbij werden vele voor kinderporno gebruikte IP-adressen via Europol en Interpol verstrekt aan verschillende landen, waaronder vier IP-adressen uit Nederland. Omdat de adressen langer dan zes maanden geleden gebruikt waren, konden de bijbehorende historische gegevens niet meer verkregen worden en kon geen onderzoek meer worden ingesteld.

Op deze wijze zijn in de afgelopen paar jaren vele tientallen meldingen en rechtshulpverzoeken betreffende Nederlandse IP-adressen die gebruikt zijn om kinderporno te uploaden of downloaden zonder gevolg gebleven omdat de zes maanden termijn om de voor onderzoek noodzakelijke historische internetgegevens te vorderen was verstreken en er geen andere aanknopingspunten waren voor onderzoek.

Daaronder bevond zich bijvoorbeeld een aangifte uit België. De ouders van een minderjarige meisje meldden de Belgische autoriteiten dat hun dochter op Habbo Hotel in een chat was benaderd door een man die vroeg of ze "zijn ding" wilde zien. Zij vertelde dat aan haar ouders en die hebben enkele dagen later op haar account ingelogd. Verdachte nam toen weer contact met haar op, vroeg of ze geil was en stelde voor op MSN te gaan. De vader is toen als zijn dochter op MSN gegaan en verdachte ging masturberend en met vieze praatjes voor de webcam zitten.
De Belgische onderzoekers kwamen via de meest recente logins op dat account uit bij enkele IP-adressen van een Nederlandse aanbieder. Op het moment dat deze informatie aan Nederland werd verstrekt konden de gegevens van het gebruikte IP-adres niet meer bevraagd worden omdat de dataretentie termijn van 6 maanden was verstreken.

Een ander voorbeeld is een melding van YouTube/Google van de upload van een schokkend filmpje (minderjarige meisje wordt seksueel misbruikt) vanaf een Nederlands IP-adres. Beeldmateriaal van dit slachtoffer was eerder in België aangetroffen en zit in de internationale database van nog onopgeloste zaken (de ICSE database van Interpol). Dit wijst op een recente, onopgeloste en mogelijk nog voortdurende misbruiksituatie. Omdat het uploaden van het filmpje langer dan zes maanden voor de melding plaatsvond, konden de gegevens van het voor de upload gebruikte IP-adres niet verkregen worden. Andere aanknopingspunten voor onderzoek zijn er niet.

---

[166] Zie http://alextimes.com/2012/10/fourth-grade-alexandria-teacher-sentence/.
[167] Zie ook Reactie van het kabinet naar aanleiding van de ongeldigverklaring van de richtlijn dataretentie, 17 november 2014, p. 7.
[168] Zie http://www.thetoc.gr/eng/news/article/hydra-operation-against-online-child-pornography.

Hoofdstuk 6. Overige vragen over de bewaarplicht en het gebruik van telecomgegevens

In dit hoofdstuk bespreken we verschillende vragen die in de discussie over de bewaarplicht aan de orde zijn gesteld en in de vorige hoofdstukken nog niet zijn besproken:

Heeft het Europese Hof de bewaarplicht niet verboden?
Nee. Het Europese Hof heeft de Europese dataretentierichtlijn ongeldig verklaard. Nederland is daardoor niet meer, zoals daarvoor, op grond van Europees recht verplicht om zijn telecomaanbieders een bewaarplicht op te leggen. Dat mag echter nog wel.

Is het wel nodig om van alle burgers alle telefoon- en internetgegevens te bewaren? Kan dat niet gerichter?
Het arrest van het Europees Hof suggereert dat de bewaarplicht beperkt zou kunnen worden tot een kring van personen van wie het gedrag 'een verband vertoont met zware criminaliteit', of tot 'gegevens die betrekking hebben op een bepaalde periode en/of een bepaalde geografische zone en/of een kring van bepaalde personen die op een of andere wijze betrokken kunnen zijn bij zware criminaliteit, of op personen voor wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij het voorkomen, opsporen of vervolgen van zware criminaliteit'.[169]
Het Europees Hof licht niet toe hoe die beperking er in de praktijk uit zou kunnen zien, en dat is ook niet eenvoudig te bedenken. Daargelaten dat een dergelijke beperking praktisch moeilijk uitvoerbaar lijkt, zou zij het nut van de bewaarplicht grotendeels teniet doen. In de hierboven aangehaalde jurisprudentie zijn in vele tientallen zaken waarbij historische telecomgegevens voor het bewijs zijn gebruikt nauwelijks voorbeelden te vinden van telecomgegevens op naam van bekende criminelen. Dat is ook logisch. Op het moment dat door de overheid met voldoende zekerheid is vastgesteld dat personen zich bezighouden met ernstige criminaliteit, zijn die personen vaak voldoende wijs geworden over de opsporing om geen 'crimineel' gebruik te maken van internet en telefoon op hun eigen naam. Misdrijven van bekende criminelen worden vooral opgelost door het gebruik van historische telecomgegevens van prepaid-telefoons en telefoons van slachtoffers en getuigen. Telefoons op naam spelen wel met regelmaat een rol, maar dat zijn dan vaak telefoons van daders die nog niet bij de overheid bekend zijn als crimineel. Voor internetgegevens geldt hetzelfde. Zulke daders die nog niet bij de overheid bekend zijn als crimineel plegen overigens wel zeer ernstige misdrijven, waaronder moord, doodslag en gewelddadige woningovervallen.
De civiele rechter heeft in zijn vonnis van 11 maart 2015 over de bewaarplicht dan ook overwogen dat een bewaarplicht voor de telecomgegevens van alle burgers op zich noodzakelijk en effectief is, en dat een beperking van de gegevens die moeten worden opgeslagen tot de gegevens van verdachte burgers niet goed denkbaar is met het oog op de doeltreffende opsporing van zware criminaliteit.[170]

---

[169] Zie arrest r.o. 58-59.
[170] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2015:2498, r.o. 3.6 t/m 3.8.

Is de mogelijkheid om telecommunicatiegegevens te laten 'bevriezen' niet een goed alternatief voor de bewaarplicht?
De mogelijkheid om telecomgegevens gericht te laten 'bevriezen' is voor de opsporing zinvol, maar - anders dan soms gesuggereerd -[171] geen alternatief voor een algemene bewaarplicht zolang de politie niet beschikt over voorspellende gaven waar, wanneer en door wie een ernstig misdrijf gepleegd gaat worden. Met 'bevriezen' worden gegevens zeker gesteld die op dat moment bij de aanbieder aanwezig zijn en later relevant kunnen zijn voor het opsporingsonderzoek. Een bevriezingsbevel zorgt ervoor dat er als het ware een foto wordt gemaakt van de situatie op het moment van bevriezing en bewaart ook alleen de situatie op dat moment. Wat niet bewaard is, kan ook niet worden bevroren.

Bij moorden, woningovervallen, verkrachtingen, het uploaden van kinderporno en tal van andere misdrijven zijn nu juist de telecomgegevens voor, tijdens en direct na het misdrijf cruciaal. Voor het vaststellen van patronen in bewegingen en contacten of relaties tussen betrokken personen zijn telecomgegevens over een langere periode voor het misdrijf belangrijk.

Als de politie eenmaal is ingelicht over een misdrijf en begint met opsporen, kan er van alles bevroren worden, maar relevante telecomgegevens van de dader zullen daar meestal niet meer bij zitten. Als de politie (prepaid)telefoons heeft gevonden die zijn gebruikt voor een liquidatie of een woningoverval kunnen de verkeersgegevens van die telefoons in de cruciale dagen en uren voor het misdrijf niet meer 'bevroren' worden. Hetzelfde geldt voor het opsporen van misdrijven die middels internet wordt gepleegd: op het moment dat een slachtoffer aangifte doet valt er niets meer te bevriezen.

Kunnen slachtoffers na een misdrijf niet zelf hun telefoongegevens aanleveren als ze dat willen?
Het op vrijwillige basis door slachtoffers van bijvoorbeeld stalking of bedreiging laten opvragen van hun telefoongegevens is geen (deel)oplossing, omdat op zulke particuliere overzichten maar een deel van de voor de politie relevante informatie staat. Zo zijn bij voorbeeld wel de uitgaande, maar niet de inkomende telefoongesprekken opgenomen in een gespecificeerde factuur en ontbreken ook de locatiegegevens.

Heeft het wel zin om telecomgegevens op te slaan als er zulke goede manieren bestaan om anoniem te communiceren?
Het argument dat juist criminelen gebruik zullen maken van de mogelijkheden die er zijn om anoniem te communiceren[172] - zodat een bewaarplicht vooral de goedwillende burger treft die niets met criminaliteit te maken heeft - vindt maar zeer ten dele bevestiging in de praktijk. Het is zeker zo dat beroepscriminelen steeds vaker gebruik maken van technische mogelijkheden om anoniem te communiceren, hetgeen de opsporing bemoeilijkt. Dat raakt echter meer de inhoud van de communicatie dan de historische verkeersgegevens. Tegelijkertijd is duidelijk dat historische telecomgegevens tot op de

[171] Zie bijv. Evaluatie van de Wet bewaarplicht telecommunicatiegegevens, kamerstukken 33 870, nr. 2, p. 10-11.
[172] Zie bijv. Evaluatie van de Wet bewaarplicht telecommunicatiegegevens, kamerstukken 33 870, nr. 2, p. 5.

dag van vandaag een grote rol spelen in de (succesvolle) opsporing en vervolging van criminaliteit, zoals blijkt uit de vele recente vonnissen in dit rapport. Dat heeft verschillende oorzaken.
In de eerste plaats worden nog steeds heel veel ernstige misdrijven gepleegd door daders die geen gebruik maken van geavanceerde techniek om ongezien te communiceren. Veel (woning)overvallen worden bijvoorbeeld gepleegd door jeugdige daders die weinig professioneel te werk gaan en veel levensdelicten worden niet gepleegd door beroepscriminelen maar vinden plaats in de relationele sfeer. Daar komt bij dat ook beroepscriminelen die grote moeite doen om ongezien te communiceren wel fouten maken die door het gebruik van historische telecomgegevens kunnen leiden tot effectieve opsporing en vervolging. De wijze waarop door de Tattoo Killers en bij de Antwerpse hotelmoord (zaak Benaouf A.) gebruikte gesloten telecomcircuits van prepaidtelefoons zijn ontdekt, ondanks de professionele voorzorgsmaatregelen van de daders, en de historische gegevens van die telefoons zijn gebruikt voor het bewijs is illustratief. Tenslotte geldt dat telecomgegevens van met name slachtoffers ook vaak van belang zijn voor de opsporing, zoals eveneens blijkt uit vele vonnissen genoemd in dit rapport, bijvoorbeeld bij levensdelicten en zedendelicten.
Het Europees Hof heeft in zijn arrest van 8 april 2014 dan ook vastgesteld, in navolging van de advocaat-generaal in zijn conclusie, dat het bestaan van geavanceerde mogelijkheden om anoniem te communiceren niet betekent dat een bewaarplicht zinloos is.[173]

Betekent het feit dat de politie tienduizenden keren per jaar historische telecomgegevens opvraagt dat van tienduizenden Nederlanders wordt gecontroleerd waar en met wie zij contact hebben gehad?
Nee. Telecomgegevens worden alleen opgevraagd door de politie als dat nodig is voor een strafrechtelijk onderzoek. In veel onderzoeken worden voor één verdachte vele vorderingen gedaan omdat veel criminelen meerdere (prepaid)telefoons gebruiken, soms wel tientallen per persoon. Zo veroordeelde de rechtbank Den Haag recentelijk een drugshandelaar in wiens woning in september 2014 veertien (14) telefoons en 2 SIM-kaarten werden gevonden.[174] Het aantal vorderingen is dus niet hetzelfde als het aantal personen over wie gegevens worden opgevraagd.

Wordt het opvragen van telecomdata voor de opsporing wel door de rechter gecontroleerd?
Ja. In strafzaken die aan de rechter worden voorgelegd, wordt in het dossier verslag gedaan van het vorderen van historische telecomgegevens. Zo zijn de afgelopen jaren tienduizenden bevragingen van telecomgegevens achteraf door de rechter gecontroleerd.

Zijn er voorbeelden bekend van lekken of misbruik van historische telecomgegevens?
Nee. In het debat over de bewaarplicht wordt veel verwezen naar de mogelijkheid van misbruik of lekken, maar in de praktijk is dat voor historische telecomgegevens in Nederland nog nooit voortgekomen. Er zijn wel persoonlijke gegevens van telecomklanten gehackt, zoals namen, adressen en creditcardgegevens, maar dat zijn geen

[173] Zie arrest r.o. 50 en conclusie AG punt 137.
[174] Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2015:1971.

historische telecomgegevens. De informatie wie de gebruiker is geweest van een IP-adres dat bij zo'n hack is gebruikt is wel een historisch telecomgegeven, en is nodig om de daders van zulke hacks te kunnen opsporen.

Over een brand bij Vodafone in 2012 meldde het Agentschap Telecom dat die brand geen grote problemen had gegeven voor politie en justitie. Is dat niet een aanwijzing dat de opsporing ook wel zonder telecomgegevens kan?
Nee. Het Agentschap Telecom hield geen toezicht op de opsporing en vervolging, maar op de naleving van de bewaarplicht door Vodafone. Het onderzoek van het Agentschap Telecom was daarom niet gericht op de invloed van de brand op opsporing en vervolging, maar had uitsluitend betrekking op de toezichthoudende taken van het AT en aldus alleen op de wijze waarop Vodafone met de gevolgen van de brand is omgegaan.
Van die brand heeft de opsporing wel degelijk hinder ondervonden. Die hinder kon echter grotendeels worden beperkt door van Vodafone gebruikers historische telefoongegevens op te vragen bij de andere telecomproviders. Als Vodafone klanten een netwerk van een andere provider gebruiken (omdat het eigen netwerk niet beschikbaar is) of met een abonnee van een andere provider bellen, zijn die gegevens (ook) bij de andere provider beschikbaar. Deze situatie is dus niet vergelijkbaar met een situatie waarin telecomgegevens helemaal niet bewaard worden: in dit geval konden veel benodigde historische telecomgegevens, dankzij de bewaarplicht, met het nodige extra werk van andere providers worden verkregen.

Bijlage bij het rapport "De bewaarplicht telecomgegevens en de opsporing" van het OM en politie van 23 maart 2015.

Algemeen

In aanvulling op het rapport worden een aantal gedetailleerde voorbeelden gegeven waaruit het belang blijkt van dataretentie en de Wet Bewaarplicht voor de opsporing en vervolging van strafbare feiten. Uit deze voorbeelden blijkt dat verkeersgegevens, locatiegegevens en gebruiksgegevens - in samenhang met andere opsporingsmethoden - enerzijds zijn gebruikt om sturing te kunnen geven aan het opsporingsonderzoek en anderzijds om verdachten te identificeren. Ook zijn voorbeelden opgenomen waarin door de beperking van de bewaartermijn tot 6 maanden voor internet gegevens en tot 12 maanden voor telefoniegegevens de opsporing juist belangrijke gegevens heeft moeten missen en daardoor niet kon worden voortgezet.

De hieronder beschreven voorbeelden van strafzaken zijn exemplarisch voor de wijze waarop in opsporingsonderzoeken wordt gewerkt. In onderzoeken wordt (afhankelijk van de specifieke casus) een samenstel van opsporingsmethoden gebruikt in onderlinge samenhang. Zowel klassieke opsporing (observatie, verhoren van getuigen, aangevers en/of verdachten, sporen op de PD, taps, het vorderen van andere historische gegevens dan telecommunicatiegegevens etc.) als opsporing door gebruikmaking van gebruikersgegevens en verkeersgegevens, van internet/telefoon communicatie leveren een wezenlijke bijdrage aan het eindresultaat. Het is niet goed mogelijk de gebruikte opsporingsmethoden in een onderzoek los van elkaar te zien. Voor het bereiken van een resultaat maar ook het uitsluiten van betrokkenheid van personen (bijvoorbeeld het controleren van een alibi) is het nodig alle mogelijke opsporingsmethoden in onderlinge samenhang aan te wenden.

Casussen

A. Stalking

Zaak A-1 (Stalking)

Een vrouw doet bij de politie aangifte van stalking. Ze wordt al ruim 5 maanden telefonisch lastig gevallen door een ex-vriend. Ze voelt zich inmiddels dermate onveilig dat ze (5 maanden nadat de stalking was begonnen) besluit aangifte te doen. Zoals vaak in zaken in de relationele sfeer is er enige tijd over het nemen van deze beslissing tot het doen van aangifte gedaan. Bij stalking is er doorgaans sprake van een hinderlijk en stelselmatig volgen gedurende een langere periode. Uit de historische verkeersgegevens van de vrouw blijkt dat er tot vijf maanden geleden sprake was van een “normaal belpatroon”. Uit de gegevens blijkt ook dat zij sinds vijf maanden echter overdag en ‘s nachts met afwisselende maar vooral zeer hoge frequentie wordt gebeld door een drietal nummers. Eén van deze nummers is alleen de eerste maand gebruikt. Dat nummer stond toen op naam van haar ex-vriend. De andere twee toestellen zijn prepaid nummers. Uit onderzoek naar de verkeersgegevens van de drie nummers blijkt later dat ook de twee prepaid nummers kunnen worden toegeschreven aan de ex-vriend, aangezien is gebleken dat alle drie nummers zijn gebruikt in dezelfde (door verdachte gebruikte) telefoon. De verkeersgegevens (in dit geval onder meer gegevens die inzicht geven in de aantallen, frequentie, duur en tijdstippen van de telefoongesprekken tussen verdachte en aangever) zijn dus belangrijk bewijsmateriaal in dit onderzoek.

Deze gegevens zijn in dit soort zaken ook van cruciaal belang om aangiften van stalking te kunnen verifiëren aan de hand van overeenkomsten in de verkeersgegevens van zowel de aangever als de verdachte. Hiermee kunnen dus ook eventueel valse aangiften onderkend worden.

B. Zedendelicten

Zaak B-1 (vervolg op zaak Robert M: onderzoek Holitna)

In november 2010 is door politieregio Amsterdam-Amstelland een onderzoek ingesteld onder de codenaam 13DOK. Dit onderzoek richt zich tegen Robert M., R. van O. en E. R., die werden verdacht van het produceren, verspreiden, uitvoeren en bezitten van kinderpornografisch materiaal en het seksueel misbruiken van zeer jonge kinderen. In het Amsterdamse onderzoek is onder de verdachten een hoeveelheid digitale gegevensdragers in beslag genomen en onderzocht. Hieruit bleek dat de verdachten vermoedelijk deel uitmaken van een internationaal netwerk van personen die kinderpornografisch beeld- en videomateriaal produceren, bezitten en verspreiden en mogelijk zeer jonge kinderen seksueel misbruiken. Om de personen die deel uitmaken van dat netwerk te identificeren, op te sporen en te vervolgen werd door de Dienst Nationale Recherche van het Korps Landelijke Politiediensten, onder leiding van het

Landelijk Parket een afzonderlijk opsporingsonderzoek met codenaam Holitna gestart. Het digitale beslag uit het Amsterdamse onderzoek bedroeg ruim 4 terabyte aan data en bevatte onder meer duizenden chatberichten, meer dan honderdduizend mails en meer dan vijftigduizend foto's.

Naar aanleiding van de analyse van de chatgesprekken werden zogenaamde quickscans opgesteld, waarin werd beschreven welke contacten een (op dat moment al dan niet geïdentificeerde) persoon vermoedelijk met M., Van O. en R. had onderhouden. Van deze quickscans zijn er vervolgens 76 aan meerdere politieregio's overgedragen met het verzoek om nader onderzoek te doen. In bijna alle gevallen kon een in de chat gebruikte gebruikersnaam worden gekoppeld aan een IP-adres, dat kon worden herleid tot een Nederlandse internet service provider. Door middel van het vorderen van gebruikersgegevens ex artikel 126na Sv bij die aanbieders konden veel Nederlandse verdachten worden geïdentificeerd.

Daarnaast zijn 1.116 processen-verbaal door tussenkomst van Europol overgedragen aan in totaal 52 landen. In bijna alle gevallen betrof de belangrijkste opsporingsindicatie een IP-adres in het buitenland. In die zaken konden bij Nederlandse aanbieders geen gebruikersgegevens worden opgevraagd. In naar aanleiding daarvan in het buitenland verrichte opsporingsonderzoeken zijn tot op heden meer dan 150 verdachten aangehouden en konden meer dan 100 kinderen uit een actuele misbruiksituatie worden bevrijd. Met uitzondering van een (zeer) beperkt aantal gevallen was een gebruikt IP-adres de enige aanwijzing die kon leiden tot de identiteit van een verdachte of een slachtoffer.

In het rapport worden reeds enkele zaken opgesomd die niet opgepakt konden worden door de teams bestrijding kinderporno en kindersekstoerisme (TBKK) door het verstrijken van de bewaartermijn van internetgegevens van 6 maanden. In aanvulling daarop kunnen ook de volgende zaken genoemd worden:

Zaak B-2 (Onderzoek uit Duitsland)
Onderzoek aangeleverd door Interpol Wiesbaden. Een Duitse undercoveragent had op Gigatribe contact gelegd met een Gigatribe-gebruiker met een Nederlands IP-adres. Hij had vanuit dat account van de Nederlander 140 bestanden gedownload. Het betrof hier zwaar materiaal, voornamelijk misbruik in incest-situaties, vaginale, orale en anale penetraties van jonge tot zeer jonge kinderen, waaronder zeer jonge peuters.
Ook hier liep het onderzoek dood vanwege het feit dat in Nederland de bewaartermijn was verlopen.

Het niet kunnen opsporen en vervolgen van de verdachten in dit soort zaken betekent niet alleen dat mogelijke bezitters van kinderpornografisch materiaal niet opgespoord zijn, maar ook dat zogenaamde "groomers" niet opgespoord zijn en door kunnen gaan met hun

handelingen. Ook eventueel achterliggend kindermisbruik, immers inherent aan het voorhanden zijn van kinderpornografisch materiaal, kan daardoor niet gesignaleerd worden, waardoor misbruiksituaties van zeer jonge slachtoffers kunnen voortduren.

Zaak B-3 (kindermisbruik via Webcam.

Een zaak die wel is opgelost is een onderzoek naar het aanzetten van minderjarigen tot het doen van seksuele handelingen voor de webcam. Daarin kon de politie dankzij de historische verkeersgegevens in combinatie met opgevraagde IP adressen uiteindelijk een verdachte aanhouden. De verdachte wisselde telkens van verblijfplaats en hij had op tal van manieren toegang tot het internet, onder meer door gebruik te maken van de internetaansluiting van andere personen uit zijn omgeving. Zonder de bewaarplicht hadden de historische verblijfplaatsen noch de actuele verblijfplaats, waar uiteindelijk de aanhouding van verdachte plaats vond, kunnen worden vastgesteld.

Zaak B-4: (via webcam afdwingen seksuele handelingen)

In dit onderzoek zijn uit onder andere de inbeslaggenomen computers van de verdachten velen slachtoffers gebleken. Nagenoeg allen meisjes tussen de 10 en 16 jaar die, doordat verdachten zich als iemand anders voordeden, werden overgehaald om seksuele handelingen te verrichten voor de webcam. Vervolgens werden enkele van de meisjes bedreigd met het openbaar maken van de opgenomen beelden door de verdachten.

Er waren 137 meisjes te onderscheiden op de computer van één verdachte, waarvan 104 meisjes geïdentificeerd konden worden en benaderd door het hele land, met name door het bevragen van IP-adressen.

Circa 40 meisjes deden aangifte. 1 verdachte gebruikte 29 emailadressen/aliassen.

Zo kon ontucht met velen en zelfs binnendringen van een meisje onder de 16 jaar bewezen worden (naast het bezit van de kinderporno door de opgenomen webcambeelden)

Zaak B-5: (verkrachting)

Een vrouw wordt door een haar onbekende man van haar fiets getrokken en verkracht. Aan de hand van de modus operandi en het signalement van de verdachte is een analyse gemaakt van mogelijk gerelateerde delicten in hetzelfde gebied. Daaruit bleek dat in het voorliggende jaar meerdere aanrandingen en verkrachtingspogingen zijn gepleegd die mogelijk aan dezelfde dader konden worden toegeschreven. Het langlopende onderzoek is met name gebaseerd op historische verkeersgegevens. Die gegevens, tot een jaar oud, in combinatie met de verklaringen van aangevers leidden uiteindelijk naar een verdachte. Dankzij die gegevens kon worden aangetoond dat de verdachte ten tijde van de delicten bij de slachtoffers in de buurt was. De gegevens zijn (ook) gebruikt om verklaringen van de verdachte en getuigen te toetsen.

Zaak B-6 (ernstig seksueel misbruik)

Een meisje van zes werd meegenomen en ernstig seksueel misbruikt. Een week later werd een verdachte aangehouden na herkenning van zijn voertuig. Tijdens het onderzoek bleek dat in het half jaar voorafgaand aan dit zeer ernstige feit meerdere soortgelijke delicten waren gepleegd. Uit de analyse van de historische verkeersgegevens van de mobiele telefoon van de verdachte bleek dat zijn telefoon bij twee andere feiten in het stralingsgebied van de zendmast in de directe omgeving van de plaats delict was geweest. De verdachte is, dankzij de verkeersgegevens, ook voor de twee andere feiten veroordeeld.

C. Cybercrime en internet fraude

Zaak C-1. (phishing fraude)
In een Belgisch rechtshulpverzoek, werd o.a. om de tenaamstellingsgegevens van een aantal Nederlandse IP-adressen gevraagd. Via deze IP-adressen had phishing fraude in België plaatsgevonden. De Belgische politie reageerde daarmee op een hausse aan internetfraude die vanuit Nederland plaatsvond. Na bevragen van de tenaamstelling bleken twee van deze IP-adressen in gebruik bij Nederlandse verdachten. Het IP-adres was het enige aanknopingspunt.
In dit geval ging er tijd voorbij voor de Belgische banken hun informatie aan de Belgische politie ter beschikking hadden gesteld. Daarnaast was er sprake van tijdsverloop in de fase van rechtshulp, tussen het moment van het opstellen in het buitenland van het rechtshulpverzoek en het moment van de uitvoering ervan door de Nederlandse politie.

Zaak C-2 (Bancaire fraude met hulp van internet)
Eind april 2014 werd vanuit het publiek-private samenwerkingsverband tussen de politie, het OM en de grootbanken (ECTF, de electronic crimes task force) een aangifte verkregen over een geval van bancaire fraude via internet die plaats vond omstreeks november 2013.
In deze casus werden op onrechtmatige wijze door de dader de identificerende gegevens bemachtigd van een persoon die gebruik maakt van internet bankieren. De dader gebruikte deze gegevens (inlog gegevens e.d.) vervolgens om geld van de rekening te halen. De bank (die haar cliënt schadeloos stelt) is benadeelde.

Op het moment dat de aangifte werd ontvangen van de bank (ongeveer 6 maanden na het plegen van het feit) was de bewaartermijn voor internet verkeersgegevens nagenoeg verlopen. Banken en andere financiële instellingen doen eerst zelf onderzoek naar (mogelijke) fraude. Vaak gaan er maanden overheen voordat patronen worden herkend en op het eerste gezicht op zichzelf staande frauduleuze handelingen aan elkaar kunnen worden gekoppeld.

Op het moment dat deze aangifte door de politie werd ontvangen, diende bovendien eerst nog te worden onderzocht en vastgesteld welke sporen van gegevens er door de plegers van het strafbare feit zijn achtergelaten. Hiervoor zijn in dit soort zaken vaak complexe technische onderzoeken noodzakelijk. Er kan daarom niet direct worden vastgesteld welke relevante gegevens dienen te worden gevorderd en bij welke internet service provider.
Op het moment dat dit wel duidelijk was, bleken geen gegevens die kunnen leiden tot de identificatie van een mogelijke verdachte, meer aanwezig te zijn door het verstrijken van de bewaartermijn van 6 maanden. Omdat het digitale spoor (het IP adres van de computer van de dader waarmee de computer van degene die gebruik maakte van internetbankieren was benaderd) het enige aanknopingspunt was richting een mogelijke verdachte is het onderzoek gestaakt.

In veel gevallen van fraude met internetbankieren is een IP-adres het enige spoor, zodat het bovenstaande voorbeeld exemplarisch is voor meerdere casussen.

Zaak C-3 (grootschalige oplichting /phishing)
Onderzoek naar een criminele organisatie die zich bezighield met oplichting/phishing waarbij een groot aantal met name oudere personen slachtoffer zijn geworden. Daarbij werd o.a. gebruik gemaakt van katvangers.
Aanleiding van het onderzoek was een aangifte van de Sociale Verzekeringsbank (SVB) welke inhield dat via vals aangevraagde DigiD-codes van een groot aantal AOW gerechtigden via de site van SVB het begunstigde rekeningnummer van hun AOW was gewijzigd. Middels onderzoeken naar de gebruikte IP-adressen zijn de verdachten geïdentificeerd. In het verdere onderzoek zijn de historische gegevens van deze IP-adressen en van de telefoons van de verdachten van groot belang geweest. Zo kon door de historische verkeersgegevens van de telefoons van één van de verdachte kon worden aangetoond dat hij bij een groot aantal van de frauduleuze geldopnames in de buurt was van de betrokken pinlocatie.

D. Mensenhandel

Zaak D-1 (gedwongen prostitutie)
In december komt er informatie binnen over een 20 jarige dame die in de periode maart t/m september van dat jaar gedwongen in de prostitutie heeft gewerkt waarbij de inkomsten van haar werkzaamheden haar werden afgenomen. Via hulpverlening had zij zich weten te ontworstelen aan haar misbruiksituatie. Door het opvragen en analyseren van de historische verkeersgegevens van het slachtoffer over een periode van 12 maanden was de politie in staat om telefoonnummers te koppelen aan een verdachte. Dankzij de verkeersgegevens werden reisbewegingen van telefoontoestellen vastgesteld. Uit de analyse bleek dat het telefoontoestel van de verdachte en het telefoontoestel van

het slachtoffer zich gelijktijdig naar diverse plaatsen in Nederland verplaatsten en in de nabijheid van het prostitutiegebied, dan wel seksclubs verbleven. Te zien was dat de telefoon van het slachtoffer op die locaties bleef en de telefoon van de verdachte dagelijks heen en weer reisde naar zijn woonplaats. Dit patroon kwam overeen met de verklaring van het slachtoffer. Uit de verkeersgegevens van verdachte en het slachtoffer bleek dat zij, gedurende langere periode, gemiddeld meer dan 50 keer per dag telefonisch contact met elkaar hadden. Dit is een fenomeen dat bij mensenhandel vaak voorkomt en wat de mate van controle die de verdachte op het slachtoffer uitoefent bevestigt. Het behoeft geen toelichting dat de verdacht ontkent en dat dergelijke zaken veelal met name dankzij de historische verkeersgegevens kunnen leiden tot een veroordeling.

E. Levensdelicten/geweldsdelicten.

Zaak E-1 (doodslag/moord).
In een grote stad wordt een man om het leven gebracht. Zijn lijk wordt in stukken gesneden teruggevonden. Uit verklaringen van getuigen blijkt dat het slachtoffer de avond van de moord werd gebeld op zijn mobiele telefoon door een persoon die aangaf dat hij voor zijn deur stond en op bezoek kwam. Het slachtoffer had geen bel aan zijn buitendeur. Bezoek kondigde zich altijd aan met een telefoontje. Aan de hand van de historische verkeersgegevens van de telefoon van het slachtoffer werd vastgesteld welke nummers die avond naar het slachtoffer hadden gebeld. Vanuit het tactisch onderzoek konden die nummers gereduceerd worden tot één enkel nummer van een mogelijke verdachte. Een tap op dit nummer leidde tot de identificatie van de verdachte die werd aangehouden. De verdachte ontkende in de zes maanden voorafgaand aan de moord bij het slachtoffer te zijn geweest. Uit de historische verkeersgegevens van de verdachte bleek het tegendeel. De suggestie van de verdachte dat anderen zijn telefoon wel eens gebruikten vond geen steun in de historische verkeersgegevens. Bovendien droeg de verdachte daarvoor geen concreet gegeven aan, zoals een naam van een persoon of personen die zijn telefoon zouden hebben kunnen gebruiken.

Zaak E-2 (gewurgde vrouw)
Een vrouw wordt gewurgd aangetroffen in haar woning. Zowel haar echtgenoot als een huisgenoot komen als mogelijke verdachte in beeld. Uit de verklaringen van de echtgenoot, die worden bevestigd door de historische verkeersgegevens en ander tactisch onderzoek, blijkt dat het niet aannemelijk is dat hij de hand heeft gehad in de dood van zijn vrouw. De echtgenoot kon zo als verdachte worden uitgesloten.
De analyse van de telefoongegevens van de huisgenoot geven echter een ander beeld. Zijn historische gegevens zijn aanleiding voor het aansluiten van taps. Een aantal contacten van de verdachte worden gehoord. Een van hen verklaart dat hij de verdachte had horen zeggen dat hij zijn hospita in de woning op de grond had zien liggen. Dit terwijl hij bij verhoor tegenover de politie volhield dat hij zijn hospita niet had gezien die

dag. De historische verkeersgegevens zijn in deze zaak van groot belang geweest voor het uitsluiten van een potentiele verdachte, voor het zicht krijgen op de werkelijke verdachte en voor het toetsen van de betrouwbaarheid van zijn verklaringen.

Zaak E-3 (dubbele moord).

Bij een dubbele moordzaak ontstond de indruk dat de verdachte mogelijk gebruik had gemaakt van de mobiele telefoons van beide slachtoffers. De verkeersgegevens van die telefoons werden voor een langere periode opgevraagd, waardoor de normale patronen in het belgedrag van slachtoffers bekend werden en afwijkingen daarin konden worden vastgesteld. Ook was te zien welke masten aangestraald werden kort nadat de moorden gepleegd waren. Van de telefoons van beide slachtoffers bleek het belgedrag ineens sterk af te wijken van het normale patroon.

Een getuige verklaarde een onbekende stem te hebben gehoord, toen die getuige de dag van de moord naar één van de slachtoffers had gebeld. De historische verkeersgegevens bevestigden dat het nummer van dat slachtoffer (de simkaart) op dat moment in een ander toestel was geplaatst.

De patronen van de verkeersgegevens van het nummer vanaf de plaatsing in het nieuwe toestel verschilden enorm van de patronen van het belgedrag van het slachtoffer. Het belgedrag kwam echter wel overeen met de patronen van het nummer dat daarvoor in het toestel van de verdachte had gezeten. Opvallend was bovendien dat beide nummers veelvuldig gebruik maakten van de mast die in de directe omgeving van de woning van de verdachte stond. Ook het nummer van het andere slachtoffer bleek na het delict een dergelijk patroon te vertonen.

Om dergelijke patronen te kunnen vaststellen is het noodzakelijk om gegevens over een langere periode op te kunnen vragen en dus te bewaren.

Zaak E-4 (dode vrouw in woning)

Een vrouw werd dood in haar woning aangetroffen. Opvallend was dat er in de woning geen mobiele telefoons werden aangetroffen. Op basis van getuige-verklaringen werd er een verdachte aangehouden.

Van zowel het slachtoffer als de aangehouden verdachte werden de historische verkeersgegevens opgevraagd. Uit de historische verkeersgegevens van de verdachte bleek echter dat zijn telefoon op het tijdstip van de moord gebruik maakte van masten elders in het land waaronder die in het gebied waar het werk van de verdachte was. Verklaringen bevestigde dat de verdachte op het tijdstip van de moord aan het werk was en de man werd vrijgelaten. In deze casus hebben de historische verkeersgegevens tot een bevestiging van het alibi geleid , zijn de verklaringen van getuigen objectief getoetst en is aldus een onschuldige als verdachte uitgesloten.

Zaak E-5 (na stalking om het leven gebrachte vrouw)

Uit de historische verkeersgegevens van een om het leven gebrachte vrouw bleek dat zij enkele uren voor haar dood ruim 50 keer was gebeld door een ander telefoonnummer. Dat nummer bleek te zijn van een man tegen wie het slachtoffer eerder aangifte had gedaan van stalking. Uit de historische verkeersgegevens van deze verdachte bleek op basis van de locatiegegevens van zijn telefoon dat hij de ochtend van de moord uit zijn huis was vertrokken in de richting van de woning van het slachtoffer. Rond het tijdstip van de moord bevond zijn telefoon zich in de omgeving van de woning van het slachtoffer en na de moord bleek de telefoon eenzelfde reisbeweging te maken als de telefoon van het slachtoffer.
Na zijn aanhouding verklaarde de verdachte dat hij het slachtoffer wel vaker veelvuldig belde en dan ook richting haar woning ging. Zo ook de ochtend van de moord. Hij verklaarde verder dat de vrouw nog leefde toen hij vertrok en dat degene die na hem was gekomen de vrouw om het leven had gebracht. Uit de historische verkeersgegevens van de verdachte bleek echter dat hij in het jaar voorafgaand aan de moord de vrouw nooit veelvuldig achter elkaar had gebeld en dat hij nooit in de ochtend naar haar toeging.

Zaak E-6 (Afpersing/vrijheidsberoving/mishandeling)

Nederland krijgt het verzoek van Zwitserland de afpersing, vrijheidsberoving en mishandeling van een Zwitsers staatsburger in Den Haag te onderzoeken en te vervolgen. Uit onderzoek blijkt dat verschillende in een Nederlands drugsonderzoek afgeluisterde telefoongesprekken gelieerd kunnen worden aan de afpersing van de Zwitser. Middels doorrechercheren op die afgetapte gesprekken kunnen alle afpersers geïdentificeerd worden op één na: die persoon gebruikte een prepaid telefoon en werd nooit bij naam genoemd in de telefonische contacten. De historische verkeersgegevens van die prepaid telefoon konden niet meer worden opgevraagd voor de periode rondom de afpersing omdat de bewaartermijn reeds was verstreken. Zou dat wel hebben gekund, dan was de kans groot dat ook deze afperser geïdentificeerd had kunnen worden. Nu blijft hij buiten beeld (het betreffende telefoonnummer blijkt inmiddels van eigenaar gewisseld), terwijl zijn collega-afpersers worden veroordeeld tot gevangenisstraffen.

Zaak E-7 (moord/doodslag)

Slachtoffer wordt op 18 januari 2013 dood in haar woning gevonden; ze is door geweld overleden. Er ontstaat zicht op een verdachte, welke verdenking wordt onderbouwd door forensisch en tactisch bewijsmateriaal en telecomonderzoek. Verdachte beroept zich vanaf het begin op zijn zwijgrecht. In februari 2014 beschikt de verdediging (en de verdachte) over het volledige dossier. Tijdens de inhoudelijke behandeling op 24 april 2014 legt verdachte ineens een verklaring af die er op neerkomt dat hij in het holst van de ochtend in zijn woning een telefoontje heeft gekregen van een man waarvan hij de naam niet wil noemen. Deze man vraagt hem naar de Zaagmuldersweg te komen (dat is in de buurt van de woning van het slachtoffer.). Daar treft verdachte bij die NN-man ook het stoffelijk overschot aan. De NN-man vraagt verdachte tegen beloning het stoffelijk

overschot op te ruimen. Verdachte tilt daarop het stoffelijk overschot op en draagt het naar de woning van het slachtoffer waar hij het (ongeveer) neerlegt zoals het werd gevonden. Dat zou volgens verdachte het forensisch sporenbeeld verklaren. Verder heeft hij ook een verhaal bij het tactische bewijsmateriaal en de bevindingen van het telecomonderzoek.

Hoewel de verklaringen van verdachte ongeloofwaardig zijn en waarschijnlijk – in ieder geval voor een gedeelte – weerlegd zullen kunnen worden door een reconstructie en hernieuwd forensisch en tactisch onderzoek, is een gegeven dat de start van zijn verhaal, dat nachtelijke telefoontje, niet geverifieerd of gefalsifieerd kan worden. Hij zou het telefoontje ontvangen hebben op een GSM en een simkaartje die niet tijdens de doorzoeking in zijn woning, in zijn fouillering of anderszins zijn gevonden en de mastgegevens over het gebied waar zijn woning staat, zijn niet bevraagd, omdat daar destijds geen aanleiding voor bestond. Die bevraging was op 24 april 2014 niet meer mogelijk vanwege het verstrijken van de bewaartermijn, maar zou objectieve aanknopingspunten hebben opgeleverd voor het controleren van de betrouwbaarheid van zijn verklaring.

Zaak E-8 (Moord Drenthe)

In het najaar van 2012 is een vermoorde man gevonden in de bossen van Zuid-Drenthe. Omdat het hier schijnbaar een "toevallig" slachtoffer betrof is een groot en langdurig onderzoek naar deze moord ingesteld. Eén van de deelprojecten van dit onderzoek betrof een onderzoek naar telecomgegevens. Aan de hand van historische verkeersgegevens, mastgegevens (en de verdere zoekslagen op telefoonnummers, masten etc) is de route van de telefoon van het slachtoffer in beeld gebracht. Het is gelukt om dit op zeer nauwkeurige wijze te doen, hetgeen een schat aan informatie opleverde. Het telecom onderzoek kan niet los worden gezien van de andere onderzoekshandelingen en nadat de verdachten op grond van andere onderzoeksresultaten waren aangehouden, bleken de resultaten van het telecom onderzoek van groot belang, onder meer om later de verklaringen van de verdachten te kunnen verifiëren en falsificeren.

Zaak E-9 (gewelddadige overval en gijzeling woning[175])

De verdachte heeft samen met een aantal anderen een gewelddadige overval gepleegd op het slachtoffer door hem komend van zijn werk in de lift nabij zijn woning onverhoeds vast te pakken, hem met een vuurwapen op het hoofd te slaan, hem tape om het hoofd en de mond te wikkelen, zijn handen te boeien en hem in zijn eigen woning gedurende meer dan een dag (26 uur) gegijzeld te houden. Het slachtoffer heeft in doodsangst zijn bankpas en pincode moeten afgeven, terwijl voorts gedreigd is bij hem een vinger af te snijden. In de woning van het slachtoffer is geld weggenomen. Voorts is met behulp van de door het slachtoffer afgegeven pincode meerdere keren en op verschillende plaatsen getracht via internetbankieren geld van de bankrekening van het slachtoffer over te

[175] http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBSGR:2011:BP5216

boeken naar de bankrekening van een katvanger. Met de door het slachtoffer afgegeven bankpas en pincode is voorts een aantal keren geld gepind en geprobeerd geld uit een pinautomaat op te nemen.

De rechtbank overweegt over het gebruik van telecomgegevens in het onderzoek:
In de onderhavige zaak heeft het openbaar ministerie zich voor zijn bewijsvoering in belangrijke mate gebaseerd op de zogenoemde historische gegevens en zendmastgegevens betreffende gsm-toestellen. In het dossier bevinden zich omvangrijke processen-verbaal waarin die zendmastgegevens en het telefoonverkeer zijn uitgewerkt en geanalyseerd. De rechtbank acht die gegevens, mede gelet op afgelegde verklaringen van de getuigen-deskundigen, voldoende betrouwbaar om als bewijs te kunnen dienen. De rechtbank neemt daarbij als uitgangspunt dat zendmastgegevens in beginsel een ondersteunend karakter hebben maar dat die gegevens in onderling verband beschouwd en in samenhang met andere uit het dossier blijkende feiten en omstandigheden voor de bewezenverklaring redengevend kunnen zijn. Daarbij betrekt de rechtbank onder meer de omstandigheid dat uit de gegevens - waaronder begrepen de gegevens zoals die op basis van de onderliggende processen-verbaal tijdens een presentatie ter terechtzitting visueel inzichtelijk zijn gemaakt - blijkt dat aan verschillende verdachten toe te schrijven gsm-toestellen zowel voor als tijdens de gijzeling (afpersing van bankpas en pincode en diefstal van geld uit de woning) onderling contact hebben, zich gelijktijdig van de ene locatie naar een andere locatie verplaatsen en/of zich gelijktijdig in het straalgebied van eenzelfde zendmast bevinden, althans in de directe omgeving van die zendmast, terwijl tevens is komen vast te staan dat die zendmast zich bevindt op of in de directe nabijheid van een van de zogenoemde "plaatsen delict" zoals aangeduid en beschreven in de processen-verbaal. Daar komt nog bij dat in een aantal gevallen ook de fysieke aanwezigheid aldaar van een of meer verdachten uit de bewijsmiddelen is komen vast te staan. Voorts staat vast dat verdachte en zijn medeverdachten [B], [C] en [D] elkaar kennen.

De rechtbank overweegt voorts:
Uit de historische verkeersgegevens van mobiele telefoonnummers die aan verdachte en zijn medeverdachten kunnen worden toegeschreven en de beschikbare zendmastgegevens kan de aanwezigheid van deze telefoonnummers in (de omgeving van) de verschillende plaatsen delict en andere relevante plaatsen, zoals bijvoorbeeld verblijfadressen van verdachten, worden afgeleid.

En:
Onder verwijzing naar hetgeen hiervoor inleidend is overwogen merkt de rechtbank op dat historische verkeersgegevens en zendmastgegevens in beginsel een ondersteunend karakter hebben. Voor zover het gaat om de gegevens van enkel verdachte neemt de rechtbank dit als uitgangspunt. De rechtbank is evenwel van oordeel dat de historische

verkeersgegevens en zendmastgegevens van verdachte en zijn medeverdachten in hun onderlinge samenhang beschouwd tezamen met andere uit het dossier blijkende feiten en omstandigheden redengevend kunnen zijn.

Zaak E-10. (meerdere malen poging doodslag)
Onderstaande casus maakt deel uit van een onderzoek, waarin bleek van een hele reeks zeer ernstige geweldsdaden uitgaande van verdachte A. Deze creëerde zoveel angst om hem heen, dat veel slachtoffers geen aangifte durfden te doen, en dat pas deden na te zijn benaderd door de politie tijdens detentie van A. Daarom konden vrijwel alle zaken slechts door 'terug rechercheren' aan het licht worden gebracht. Telecomgegevens, voor zover nog voorhanden, speelden daarin een zeer belangrijke rol. In onderstaande casus speelden telecomgegevens van meer dan 6 maanden oud een cruciale rol.

Als uitvloeisel van een langer lopend conflict nodigt A het slachtoffer uit om thuis een geldbedrag te komen ophalen. A nodigt echter ook een aantal relaties, 'soldaten', uit die de straat en omgeving verkennen. Als het slachtoffer tezamen met enkele vrienden verschijnt en bemerkt dat het niet pluis is, loopt hij gauw door. Er ontstaat op straat echter een handgemeen tussen het slachtoffer en een relatie (die volgens het slachtoffer voorzien is van een uzi) van A. Als het slachtoffer een paralyser pakt, wordt hij met een pistool beschoten door A. Hij wordt geraakt in een been, weet weg te komen, en geneest. Maar hij durft niet naar een dokter en doet geen aangifte.

Maanden later, naar aanleiding van een andere poging tot doodslag door A, vertelt een vriendin van A gehoord te hebben van diens betrokkenheid bij het hiervoor genoemde. Met moeite achterhaalt de politie de identiteit van het slachtoffer, die – nu A inmiddels vastzit voor iets anders en nu de politie al wat blijkt te weten – alsnog wil praten en na bijna 6 maanden alsnog naar een dokter durft.

Hierna doet de politie uitgebreid onderzoek naar onder meer de andere aanwezigen, zowel van de zijde van A als van het slachtoffer. Op basis van de mastverkeersgegevens en overige telecomgegevens komen telefoonnummers van een aantal mannen in beeld die rond het moment van het schieten aanstralen op een mast in de buurt van de plaats van het delict en die contact hadden met de telefoon van A. Zij worden achterhaald en geconfronteerd met de aanwezigheid van hun telefoon op deze plaats en tijd. Mede door hun verklaringen komt duidelijkheid over deze schietpartij op de openbare weg. Dat zou niet mogelijk zijn geweest zonder de telecomgegevens die voor het grootste deel tussen 6 en 12 maanden oud waren.

Zaak E 11. (woningoverval en verkrachting)
Bij thuiskomst overloopt de vrouw des huizes twee inbrekers, waarna zij door de inbrekers een uur of twee gekneveld in haar eigen huis gegijzeld wordt gehouden.

Wanneer de inbrekers lijken weg te gaan komt een van de mannen terug en wordt zij, terwijl ze nog steeds gekneveld ligt, door deze inbreker verkracht. Deze zaak biedt, op een DNA-sperma spoor na, nauwelijks aanknopingspunten.
Het DNA matcht echter met een DNA daderspoor van een overval op een woning van ongeveer een half jaar eerder. Die zaak levert aanknopingspunten voor telefoongegevens. Via historische verkeersgegevens en mastverkeersgegevens afgeleid uit die oudere zaak is uiteindelijk pas zicht ontstaan op de verdachte die ook de verkrachting heeft gepleegd.
Als het niet mogelijk was geweest oudere telecomgegevens op te vragen, zou de verkrachter niet opgespoord zijn.

F. Brandstichtingen

Zaak F-1: (brandstichting bij een woning)
In een onderzoek naar brandstichting bij een woning waar een oudere vrouw lag te slapen, kwam het onderzoeksteam de verdachten pas op het spoor nadat er telefoontaps waren gezet en zich uiteindelijk een tipgever heeft gemeld. Pas op dat moment – enkele maanden later – konden de historische verkeersgegevens van deze verdachten worden opgevraagd om zo te onderzoeken of zij de desbetreffende avonden rondom de plaats delict waren geweest, of bijvoorbeeld kort daarvoor of vlak daarna.Tevens gaf een van deze verdachten (3/4 jaar na de brandstichting) een alibi op dat later – na vergelijking van de historische verkeersgegevens – niet bleek te kloppen.

Zaak F-2 Onderzoek naar seriematige brandstichtingen.
Het duurde enige tijd voordat het vermoeden ontstond dat meerdere branden die geografisch verspreid plaatsvonden, wellicht door een en dezelfde persoon waren gepleegd. Een lang en tijdrovend onderzoek heeft geleid tot het in kaart brengen van patronen in het gedrag van een verdachte. Dat had niet kunnen gebeuren als de historische gegevens van zijn telefoon niet bewaard gebleven waren. Op basis van de historische gegevens lukte het om in kaart te brengen dat de telefoon van verdachte bij al die branden in de buurt was, hetgeen uiteindelijk in belangrijke mate heeft bijgedragen aan het bewijs. Zonder het kunnen opvragen van telecomgegevens over een langere periode was het niet gelukt om deze seriebrandstichter te pakken en veroordeeld te krijgen.

G. Overige zaken

Voorbeeld G-1: (poging afpersing grote landelijke bank, bommelding)
Poging afpersing van een bank in het oosten van het land in april 2013, waaronder een dreiging met een bom die geplaatst zou zijn. De melding had een grote impact. De bank en een deel van de binnenstad werden een groot deel van de dag ontruimd en afgezet. Deze zaak kon alleen worden opgelost dankzij historische telefoongegevens .

Er kon door eerst gebruikersgegevens op te vragen, worden achterhaald waar de prepaid sim-kaarten van de telefoons waarmee de dreigberichten per sms aan de directeur van de bank werden verzonden, zijn uitgegeven en op welk moment ze zijn geactiveerd. Middels opgevraagde camerabeelden kwam de man in beeld die deze sim-kaarten bij een tankstation heeft aangeschaft. Deze beelden werden vertoond in Opsporing Verzocht en in Onder de Loep. Hierop kwamen meerdere reacties binnen die allemaal verwezen naar een specifieke verdachte.
Uit de politiesystemen bleek dat hij sinds enige jaren in het buitenland woonde. Een Europees aanhoudingsbevel werd uitgevaardigd, alsmede een rechtshulpverzoek om bij de aanhouding ook een doorzoeking van de woning te laten verrichten door de buitenlandse autoriteiten. De aanhouding en doorzoeking vonden plaats op 5 november 2013. Op 3 januari 2014 werd verdachte door de autoriteiten uitgeleverd aan de Nederlandse politie. Pas op dat moment kon verdachte worden verhoord, nieuwe gegevens verzameld en worden vergeleken en onderzoek worden gedaan aan inbeslaggenomen goederen.

Na alle bewijsvoering heeft de steeds ontkennende verdachte uiteindelijk pas ter zitting bekend.

Zaak G-2: (Bedreiging)
In februari 2013 wordt er aangifte gedaan van bedreiging. Het slachtoffer werd middels SMS-berichten duidelijk gemaakt dat zij seks moest hebben anders zou zij en een aantal met name genoemde vriendinnen van aangeefster verkracht worden door een aantal personen. Aangeefster moest binnen een week reageren. In een van de SMS-berichten stond dat er iets in de brievenbus van aangeefster zou liggen. Toen aangeefster dit controleerde, zag zij in de brievenbus een envelop liggen met haar naam er op. In de enveloppe zaten foto's van pistolen en steekwapens. Twee maanden later deed een andere vrouw aangifte van een identiek feit waarbij de SMS-berichten van een andere telefoonnummer werden verstuurd.
Van beide telefoonnummers werden de historische verkeersgegevens opgevraagd over een periode van drie maanden. Hieruit bleek dat beide nummers gebruikt waren in dezelfde telefoon. Ook bleek dat er zelden gebruik werd gemaakt van de telefoon maar dat er wel meerdere inbellende contacten waren geweest op één van de gebruikte mobiele nummers door een vast telefoonnummer van een transportbedrijf. Uit de verkeersgegevens konden op één dag in het bijzonder bepaalde reisbewegingen van het toestel worden vastgesteld. De combinatie van de verkeersgegevens en de bij het transportbedrijf gevorderde informatie leidde naar de verdachte van deze bedreigingen. De verdachte is een medewerker van het transportbedrijf.

Zaak G-3. (Shouldering)

In Den Haag werd een vrouwelijke verdachte op heterdaad aangehouden. Zij maakte zich schuldig aan shouldering. Shouldering is het afkijken bij veelal oudere mensen tijdens het pinnen om vervolgens met een listige kunstgreep, of desnoods met geweld, het pinpasje van het slachtoffer te bemachtigen om daarmee grote bedragen te pinnen van de rekening van het slachtoffer. Bekend was dat deze werkwijze in het hele land in sterk toenemende mate werd toegepast.
Tijdens de aanhouding werd bij de verdachte een telefoon in beslag genomen. Aan de hand van de opgevraagde historische verkeersgegevens kon in kaart worden gebracht op welke dagen de verdachte op pad ging om slachtoffers te maken, en wie haar `partner in crime` was. Op basis van de verkeersgegevens kon gericht gezocht worden naar aangiften in bepaalde gebieden waardoor er aan de verdachten 8 respectievelijk 15 feiten konden worden gekoppeld. Om dergelijke patronen (contacten en locatie) te kunnen vaststellen is het noodzakelijk om gegevens over een langere periode op te vragen en dus te bewaren.

Zaak G-4 (aantonen criminele organisatie)
In een onderzoek naar een criminele organisatie worden bij de doorzoekingen (welke in grootschalige onderzoeken per definitie pas na langere tijd plaatsvinden) bij de vijf hoofdverdachten 7 a 8 prepaid telefoons gevonden waarvan de nummers niet eerder in het onderzoek bekend waren. Historische verkeersgegevens op deze telefoons en enkele andere in het onderzoek al wel bekende telefoons bewijzen dat de verdachten in het jaar voorafgaand aan de doorzoekingen onderling veelvuldig contact met elkaar hadden, hetgeen belangrijk is voor het bewijs dat zij met elkaar een criminele/terroristische organisatie vormden. Zonder telecomgegevens over een langere periode hadden we dat niet kunnen vaststellen.

H. Vermogensdelicten

Zaak H-1 (Bedrijfsinbraken)
In het zuiden van het land wordt onderzoek gedaan naar grootschalige bedrijfsinbraken. Uit de analyse van de mastverkeersgegevens van de locaties ten tijde van de inbraken komt een aantal mobiele nummers naar voren. Deze nummers, die veelvuldig onderling contact maken tijdens de delicten komen echter niet terug in de verkeersgegevens in onderzoeken naar de meest recente inbraken en evenmin bij oudere inbraken met dezelfde modus operandi. De indruk bestaat dat de verdachten periodiek hun telefoons vervingen. Uit de analyse van de nummers komt ook een vast nummer dat regelmatig contact heeft met een aantal van de mobiele nummers. Via de verkeersgegevens van dat nummer konden de oude maar ook de nieuwe nummers van de verdachten achterhaald worden en aan elkaar gekoppeld, hetgeen uiteindelijk heeft geleid tot hun aanhouding en een vervolging voor grootschalige inbraken die gedurende een jaar werden gepleegd.

Zaak H-2 Transportcriminaliteit.

In zijn algemeenheid wordt bij de aanpak van transportcriminaliteit (zowel ladingdiefstallen als bij diefstal van lading en vrachtwagencombinaties) in vrijwel alle zaken (buiten de echte heterdaadzaken) gebruik gemaakt van mast- en verkeersgegevens. De rondtrekkende criminele bendes die zich schuldig maken aan deze strafbare feiten, maken vrijwel standaard gebruik van prepaid telefoons, waarmee ze alleen elkaar bellen. Er wordt door deze groeperingen gebruik gemaakt van “verkenners” die vrachtwagens openmaken en kijken of er lading in zit en vervolgens contact opnemen met anderen om de lading op te halen met een ander voertuig. Hierbij stralen de telefoons vaak masten aan op of in de nabije omgeving van de parkeerplaatsen waar de goederen uit de vrachtauto’s gestolen worden. Tijdens een actiedag worden bij doorzoekingen vaak nog meer telefoons en/of simkaartjes aangetroffen die na onderzoek van historische print- en mastgegevens ook weer te linken zijn aan ladingdiefstallen. In een aantal projectmatige zaken heeft dit geleid tot het oplossen van veel feiten en tot lange gevangenisstraffen. Het ladingdiefstallenteam is met deze werkwijze in het verleden erg succesvol geweest, hetgeen heeft geleid tot een forse daling van het aantal gevallen van ladingdiefstal.

I. Gewelddadige overvallen.

Zaak I-1 (woningoverval)

Tijdens een overval in een woning in het zuiden van het land, waarbij geweld wordt gebruikt tegen de bewoners, waaronder kinderen, worden de overvallers gestoord door de deurbel. Er wordt gezien dat één van de overvallers in huis gebruik maakt van zijn mobiele telefoon. De onbekende overvallers slaan op de vlucht en worden op dat moment niet achterhaald. Het slachtoffer van de overval gaf, in zijn verklaring bij de politie, ook aan dat hij in de dagen voorafgaand aan de overval van zijn werk naar zijn huis een aantal malen was gevolgd door iemand in een auto.

In het opsporingsonderzoek werden de verkeersgegevens van de masten die dekking hadden bij de woning van het slachtoffer ten tijde van het gepleegde delict, opgevraagd. Deze gegevens zijn vergeleken met de tevens opgevraagde verkeersgegevens van de masten langs en ten tijde van de route die het slachtoffer van zijn werk naar huis aflegde.

Uit de vergelijking van deze gegevens uit de periode dat slachtoffer zich gevolgd waande, kwamen meerdere telefoonnummers naar voren die op alle lijsten voorkwamen. Van deze specifieke telefoonnummers zijn de verkeersgegevens over een langere periode opgevraagd om bepaalde patronen en eventuele afwijkingen daarop te kunnen vaststellen. Indien slechts de gegevens van de voor de overval relevante data worden opgevraagd, kunnen immers geen patronen worden ontdekt in vergelijking met “gewone” dagen.

Uit de analyse van de historische verkeersgegevens, inclusief de locatiegegevens, bleek dat één telefoon zich in de bevraagde periode altijd in het westen van het land bevond met uitzondering van de momenten (dagen en tijdvak) waarop het slachtoffer had aangegeven te zijn gevolgd van werk naar woning alsmede ten tijde van de overval.

Uit de verkeersgegevens van de andere nummers bleek dat het “belgedrag” ten tijde van het volgen en de inbraak niet anders was dan op andere momenten in de tijd.
Om dergelijke patronen (afwijkend belgedrag of locatie) te kunnen vaststellen is het noodzakelijk om gegevens over een langere periode op te vragen en dus te bewaren.
Door de verkeersgegevens van de zendmasten en de historische verkeersgegevens van het specifieke telefoonnummer te vergelijken met de overige opsporingsresultaten is stap voor stap zicht ontstaan op de verdachten. Hierna was het mogelijk weer verder te rechercheren op historische verkeersgegevens van medeverdachten. Het onderzoek is dan een aantal maanden verder sinds dag waarop de overval is gepleegd. Zonder deze telecommunicatie gegevens zou dit zicht op de verdachten zeer waarschijnlijk niet zijn ontstaan. De patronen in het belgedrag en met name de locatiegegevens daarvan zijn cruciaal geweest om potentiele betrokkenen als verdachte te kunnen aanmerken of juist uit te kunnen sluiten. Door de locatiegegevens zowel vanuit de historische verkeersgegevens op een telefoonnummer als de historische verkeersgegevens van de zendmast te analyseren, kon tevens de ontkennende verklaring van de verdachte over waar hij zich ten tijde van de voorverkenning (het volgen van het slachtoffer) en de overval ophield weerlegd worden. Deze verklaring van verdachten is pas na geruime tijd in het onderzoek verkregen. Aldus hebben de telecommunicatiegegevens ook een rol gespeeld voor de bewijsvoering.

In onderstaande zaken is op een vergelijkbare wijze, en dus in meerdere stappen met het vaststellen van patronen in eerst de opgevraagde mastverkeersgegevens en vervolgens relevante historische verkeersgegevens over een langere periode uiteindelijk zicht ontstaan op de verdachten. Deze methode is exemplarisch voor zaken die aanvangen met slechts een indicatie dat er een telefoon op de plaats delict is gebruikt en er mastverkeersgegevens worden bevraagd. Deze voorbeelden zijn daarom in enkele gevallen korter beschreven.

Vanuit zowel politie als officieren van justitie zijn voorbeelden van bijzonder gewelddadige woningovervallen ontvangen, waarbij, nagenoeg zonder uitzondering, de combinatie van mastverkeersgegevens, gebruikersgegevens en historische verkeersgegevens over een langere periode doorslaggevend zijn geweest voor de richting van het opsporingsonderzoek en (vervolgens) de identificatie van de daders.

Zaak I-2. (overval café)
Bij een overval op een café in Gelderland waarbij grof geweld is gebruikt tegen de twee slachtoffers is de verdachte in beeld gekomen door camerabeelden te vergelijken met telefoongegevens. Op de beelden was zichtbaar dat een van de daders iets deed met zijn telefoon (waarschijnlijk in contact blijven met de andere daders) en door de mastverkeersgegevens en het analyseren daarvan werd duidelijk welk nummer bij die persoon hoorde. Hiermee kreeg het team het – eerste – zicht op een van de daders. Vanuit

dat telefoonnummer is het team door gaan rechercheren door onder meer van bepaalde contacten van die eerste dader ook historische verkeersgegevens op te vragen en (vervolgens) uit gekomen bij vier verdachten die alle vier zijn veroordeeld.

Zaak I-3. (woningoverval)

Bij een zwaardere woningoverval kon uit de mastgegevens worden afgeleid dat de telefoons van de tipgevers van de overval de dagen voor de overval over een relevante zendmast in Rotterdam kwamen, terwijl dat eerder niet het geval was. Deze gegevens ondersteunden de verklaring van een van de daders die later vertelde hoe het was gegaan. De twee ontkennende verdachten zijn beide veroordeeld, onder andere omdat de telefoon van deze personen in Rotterdam over de relevante zendmast kwam.

Zaak I-4: (woningoverval met dodelijk slachtoffer)

Dit jaar komt een slachtoffer te overlijden bij overval op een woning. Uit verklaringen van de medebewoner blijkt dat een van de verdachten tijdens de overval een pinpas heeft gestolen en daarmee is gaan pinnen. Er zijn indicaties dat de overvallers met elkaar hebben gebeld tijdens de overval. Onderwerp van gesprek lijkt de afgedwongen pincode te zijn.

De mastverkeersgegevens van de periode gedurende de overval worden opgevraagd. Echter, in 20 minuten blijken er meer dan 500 gesprekken te zijn. Daar zouden de twee telefoonnummers van de overvallers tussen moeten zitten. Zonder nadere gegevens in eerste instantie een speld in een hooiberg.

Onderzoek naar overvallen met een soortgelijke manier van werken levert een vergelijkbare zaak op, bijna een jaar eerder. Er worden mastverkeersgegevens opgevraagd over de route die de overvallers vermoedelijk hebben afgelegd op de vlucht ten tijde van die overval.

Uit een vergelijking tussen de twee bestanden van mastverkeersgegevens van zowel de eerste als de tweede overval blijkt als opvallende overeenkomst dat er één telefoonnummer in beide bestanden voorkomt. Van dat nummer worden vervolgens historische verkeersgegevens opgevraagd over een periode die beide overvallen bestrijkt (daarvoor zijn dus de gegevens van 12 maanden noodzakelijk). Uit de analyse van deze historische gegevens blijkt dat rond het tijdstip van de recente overval met dat telefoonnummer inderdaad contact is met een ander telefoonnummer dat ook voorkomt op de mastverkeersgegevens van masten die worden aangestraald vanaf de plaats delict (dat dus heel wel het nummer van een van de overvallers kan zijn) en bovendien veel contact heeft op die dag met enkele buitenlandse telefoonnummers.

Rechtshulp is noodzakelijk – en dus tijdverlies – om de gebruikers van die nummers te achterhalen. Vergelijking van foto's verkregen uit het buitenland met foto's van o.a. de camerabeelden uit het onderzoek naar de recente overval levert 3 verdachten op.

Met de resultaten van dit telecom-onderzoek is inmiddels ook een groot deel van het bewijs in deze zaak geleverd.

Zonder gebruik van de telecommunicatie gegevens zou:

- Er niet de opsporingsindicatie (kansen) geweest zijn die er nu was;
- Uit de 500 gesprekken in de periode rond de recente overval nooit het juiste gesprek van de overvallers snel geselecteerd kunnen zijn;
- De link met de eerste overval niet gelegd kunnen worden;
- De link naar de buitenlandse nummers niet in beeld zou zijn gekomen;
- De gebruikers van de telefoons van de overval via een rechtshulpverzoek niet zijn geïdentificeerd;
- Het bewijs niet – min of meer – al rond zijn geweest voor de aanhouding.

Zaak I-5: (woninginbraak met vuurwapengeweld)

Zaak in het westen van het land tegen vier gewelddadige verdachten bij een woninginbraak waarbij met een doorgeladen vuurwapen met de politie is gevochten en de honden van de bewoners doorzeefd met kogels werden aangetroffen. De leidinggevende “vijfde man” is later aangehouden kunnen worden na analyse van de telefoongegevens van de telefoonnummers van de eerste vier aangehouden mannen. Die analyse van de locatiegegevens liet bovendien heel duidelijk zien hoe de telefoon van de “vijfde man” zich meermalen verplaatste naar de toenmalige woonplaats van een van de verdachten in België. Om dit beeld te kunnen schetsen zijn historische verkeersgegevens over langere periodes noodzakelijk geweest, waarvan de analyse steeds de nodige tijd in beslag heeft genomen.

Naar overtuiging van de behandelend officier van justitie had de leidinggevende 5e persoon niet geïdentificeerd kunnen worden als niet historische telecomgegevens over een lange periode hadden kunnen worden opgevraagd. In combinatie met een analyse van real-time verkeersgegevens is de vijfde man ook daadwerkelijk aangehouden kunnen worden. Telecommunicatiegegevens over een langere termijn zijn in deze zaak dus cruciaal geweest om de leidinggevende verdachte te kunnen identificeren en aanhouden.

Zaak I-6 (overval van bedrijf).

Een bedrijf wordt met veel geweld overvallen. De medewerkers en de eigenaar leggen geëmotioneerd verklaringen af. Uit analyse van de mastverkeersgegevens, in combinatie met de verklaringen van slachtoffers en getuigen komt een nummer naar voren dat mogelijk betrokken is bij de overval. Dat nummer wordt, op het moment dat het ter kennis van de politie komt, al niet meer gebruikt.

Dat telefoonnummer heeft, blijkens de historische verkeersgegevens, een aantal dagen voor de overval meerdere keren contact gehad met een bepaald bedrijf. Uit de bij dat bedrijf gevorderde gegevens volgt de identiteit van degene die ten tijde van de overval het telefoonnummer in gebruik had. Dat blijkt namelijk een medewerker van dat bedrijf

te zijn. Verder onderzoek leidde naar andere telefoonnummers in gebruik bij deze verdachte. De combinatie van de analyse van de verkeersgegevens van die nummers en andere informatie bracht de medeverdachten in beeld.
Het onderzoeksteam is van oordeel dat zonder de historische verkeersgegevens deze zaak nooit was opgelost.

Zaak I-7 (overval in een woning)
In een dorp wordt een gezin overvallen in hun boerderij. De overvallers zijn na flink wat geweld te hebben gebruikt niet tevreden met de opbrengst van de overval en bellen vanuit de boerderij met een handlanger om te vragen of er niet meer moet zijn. De mastverkeersgegevens worden opgevraagd.
Een week later vindt er een soortgelijke overval plaats in een stad. Hierbij worden ook de mastverkeersgegevens opgevraagd. De gegevens van beide overvallen worden met elkaar vergeleken en er komt één gemeenschappelijk nummer uit.
Na de analyse van de historische verkeersgegevens van dat nummer kan de identiteit van de gebruiker van dat nummer worden vastgesteld. Tijdens de aanhouding treft de politie onder het kussen van de verdachte een doorgeladen vuurwapen aan.

Zaak I-8 (gewapende woningoverval)
Betreft onderzoek naar een gewapende woningoverval door vier gemaskerde mannen. In de woning was aanwezig een gezin met vier jonge kinderen. Bij de vlucht is geschoten. Bij dit schietincident is één van de verdachten gewond geraakt. Dankzij DNA is hij kort hierop aangehouden. O.a. door gebruik van de maskers en handschoenen zijn er van de overige drie verdachten geen fysieke sporen aangetroffen. De aangehouden verdachte wil niets verklaren over zijn mededaders.
In het onderzoek zijn onder meer de mastverkeersgegevens opgevraagd van de locatie van de woningoverval en die waar de vluchtauto is gevonden. Daarnaast zijn historische verkeersgegevens opgevraagd van de telefoon van de aangehouden verdachte en nummers die uit de analyse van de mastverkeersgegevens naar voren waren gekomen. Dankzij een grondige analyse van deze gegevens is het gelukt de overige drie verdachten te identificeren. Daarbij was de termijn van de opgevraagde telecomgegevens ook van belang. Door gegevens op te vragen over een langere periode konden namelijk terugkerende contacten worden vastgesteld (meest gekozen nummers) wat vervolgens weer aanknopingspunten opleverde voor verder onderzoek. Klassieke opsporingsmiddelen leverden in deze casus juist geen verdere aanknopingspunten op.